Influence of Cyber Risk on the P&C Insurance Market

Edmund D Douglas, FCAS, MAAA

June 2016

Willis Towers Watson

Agenda

- Cyber Risk and Fire Risk – the Parallels
- State of P&C Insurance Market
- Factors Driving the Demand
- Response From Insurers
- Ideas Proposed to Increase Market Penetration

Cyber Risk and Fire Risk – the Parallels

Past State of Affairs of Fire Risk

- **This year is the 350th anniversary of the Great Fire of London**
  - One of the largest urban fires in history
  - Destroyed a third of the city and resulted in 100,000 homeless
- **Increased fire risk was a significant negative consequence of urbanization**
  - Risks that came with urban expansion were serious, but did not dissuade people from city living
  - Instead, society captured the massive benefits through risk mitigation, including insurance
- **Response to the risk of urban fire was multifaceted, where every intervention made was necessary, and none was sufficient on its own**
  - Governments required building in brick and stone, not wood
  - Local authorities established fire brigades
  - People stopped heating with open fires in their homes
  - Fire insurance was developed

Current State of Affairs of Cyber Risk

- **Increased cyber risk is a significant negative consequence of the digital revolution**
  - But should it dissuade society from becoming more interconnected?
  - There are many benefits that society may reap from Internet of Things (IoT)
- **Sounds very similar to the situation with fire risk and urbanization**
- **Response to cyber risk will likely be very similar to that of urban fire risk**
  - Multifaceted, where a number of interventions will be necessary – none of which will be sufficient on its own
  - Proactive risk mitigation will lead to lead to reduced risk

Putting It All in Perspective

Fire Risk – *past*	**Cyber Risk** - *current*
▪ Significant and complex risk to manage due to urbanization	▪ Same as fire risk, except due to digitalization and IoT
▪ Major event could disable critical infrastructure, imperil national security and threaten the economy	▪ Same as fire risk
▪ In spite of the risk people still gravitated towards city living	▪ In spite of the risk people and businesses are gravitating towards a more interconnected world
▪ Response to the risk involved an integrated approach involving public, private and social sectors adopting a package of risk mitigation measures	▪ Stay tuned…

State of P&C Insurance Market

State of the P&C Insurance Market

Growth challenges faced by insurers in recent years	Capital levels for the industry are at all-time highs and continue to rise	Product supply outpacing demand for many insurance products	A few exceptions exhibit potential for high growth
Driver of recent wave of M&A transactions and stock buybacks	But identifying attractive opportunities for deploying capital has been difficult	Resulting in limited opportunities for organic growth	Insurance solutions for Cyber Risk

An Opportune Time for P&C Insurance Market

- Cyber risk is increasing, and so is the demand for comprehensive cyber risk solutions
- At last, an opportunity for organic growth for the P&C industry in what is challenging growth environment
- Insurers have certainly responded with various cyber products
  - However, there are significant challenges that constrain their ability to fully penetrate this market

Factors Driving Demand

Major cyber breach events since 2014

Date	Company Affected	Number of records effected	Type of information stolen	Total costs incurred	Insurance cover	Total cost/ Market Cap*
Feb 2015	**Anthem**	**80 million**	Names, Social Security numbers and other personal information	US$230 million[1]	Cyber coverage between US$150-US$200 million	0.63%
Nov 2014	**Sony**	**47,000**	Social Security numbers	Estimated to be around US$100 million	100% covered by insurance	0.32%[2]
Oct 2014	**JPMorgan Chase**	**76 million household, 7 million businesses**	Customer names, Addresses, Phone numbers and Email addresses	-[3]	-	-
Sep 2014	**Home Depot**	**56 million**	Credit and Debit card information	US$232 million[4]	US$30 million	0.17%
Aug 2014	**Community Health Systems**	**4.5 million**	Patient names, birth dates, addresses, telephone and social security numbers	-[5]	-	-
Dec 2013-Jan 2014	**Target**	**40 million**	Credit and debit card information	US$290 million	US$90 million	0.81%

*Market cap in USD millions as at end of fiscal year of the breach, as sourced from Bloomberg.

1. Figure as of Dec 2015. It is reported that most of its costs were covered by the company's cyber insurance policy.
2. The US$100 million on which this is calculated is a third party estimate. Sony has not released any data regarding the data breach losses incurred.
3.,5. The company has not released data breach related costs in its latest annual report.
4. Costs as reported in October 2015.

Major cyber breach events (continued)

Date	Company Affected	Number of records effected	Type of information stolen	Total costs incurred	Insurance cover	Total cost/ Market Cap*
Jul-Aug 2015	**Ashley Madison**	**32 million**	Names, Addresses, phone numbers and credit card information	£1.2 billion[1]	-	-
Jan 2015[2]	**Premera Blue Cross**	**11 million**	Name, Social security number, telephone number, medical information etc.	-	-	-
Sep 2015	**Excellus BlueCross BlueShield**	**10.5 million**	Name, Social security number, telephone number, medical information etc.	US$17.3 million[3]	US$9.1 million	-
Sep 2015	**Experian**	**15 million**	Names, addresses, social security, driver's license and passport numbers	US$20 million[4]	US$10 million[5]	0.12%
Dec 2015	**United States voters**	**191 million**	Name, address, birth dates, phone numbers and emails	-[6]	-	-
Jul 2015	**Korea Pharmaceutical Information Center**	**43 million[7]**	Medical health information on patients in Korea	-	-	-

*Market cap in USD millions as at end of fiscal year of the breach, as sourced from Bloomberg.

1. Estimated damages that the Canada-based company faces in the UK only from class action lawsuit. Global damages expected to be much more.

2. Discovered in Jan 2015, the cyber attack actually took placed in May 2014.

3. Costs reported as of 2015. Costs incurred for 2016 have not been released yet.

4. Costs reported till Nov 2015. The company expects further damages related to possible lawsuits.

5. Though no insurance cover amount could be sourced, insurance cover is expected to take care of 'short term' costs of the breach like customer notifications, which were pegged at US$10 million by analysts.

6. The data was attributed to accidental loss due to a misconfigured database and no damages were reported.

7. Represents nearly 90% of Korea's population. Although this insider data breach is under investigation, no costs have been reported so far.

Recent Cybersecurity Incidents

Data breaches have been happening at a disturbingly frequent rate

- Due to increased reporting of breaches that happened before but were not disclosed?
- Due to increased activity by, and effectiveness of hackers?

Leading many businesses to re-evaluate their expectations

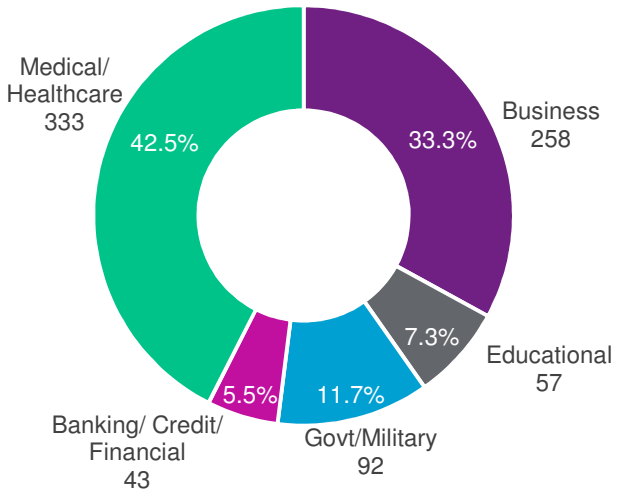
- More a matter of when a breach occurs, rather than if a breach occurs

Other Factors Driving Demand

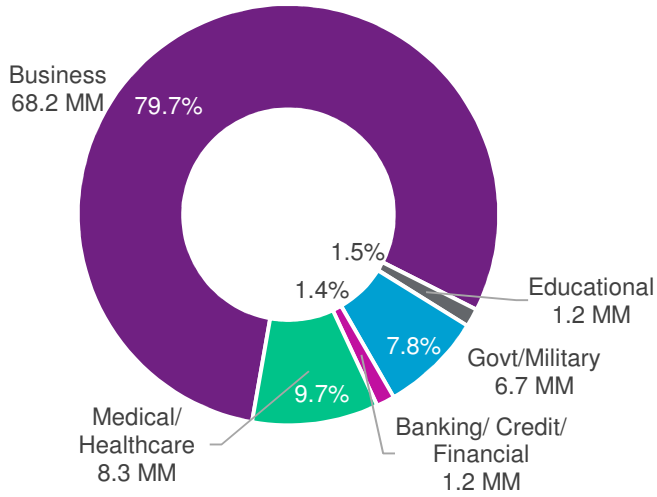
- Vendor requirements, particularly for small and mid-sized (SME) companies
  - Customers, clients, suppliers, lenders may refuse to do business with a SME if cyber-insurance is not in place
- Regulatory pressures, which encourage the use of cyber-insurance
- Stricter privacy notification laws
- Traditional insurance policy exclusions

Data Breaches by Business Category

2014 Data Breaches By Business Category, By Number of Breaches



2014 Data Breaches By Category, By Number of Records Exposed



Source: Identity Theft Resource Center

Response From Insurers

Insurers Have Responded Very Cautiously

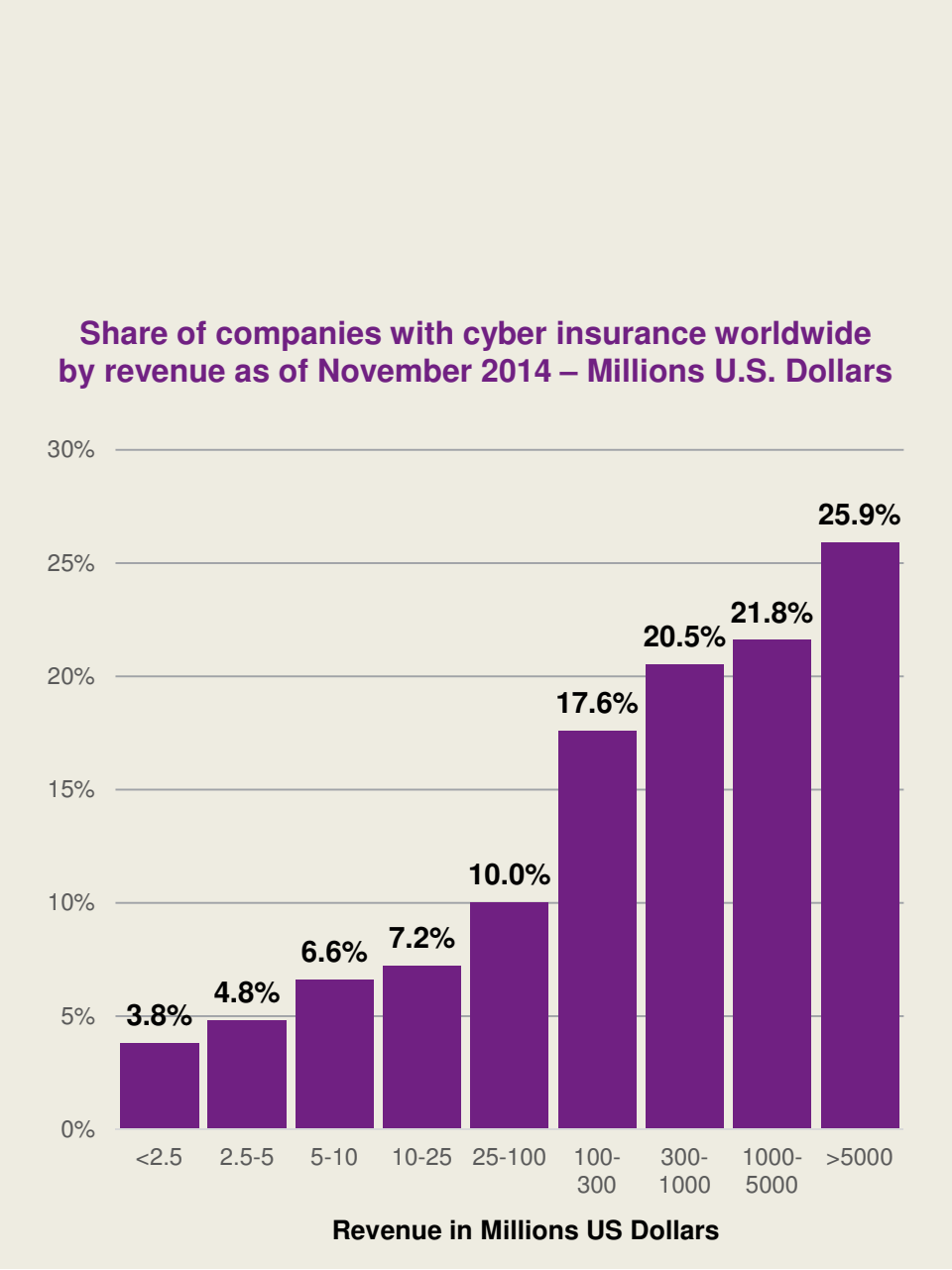
- Cyber-crime is evolving at a very fast pace
  - Perpetrators have advanced capabilities and are continuously devising sophisticated tools to breach security systems
  - Also contributing is the Internet of Things (IoT) – increased use of cloud computing and evolution in mobile technology
- Historical data is very limited, especially since past data is unlikely to be predictive of the future
  - As a consequence of the limited historical claims, few precedents exist to handle potential coverage disputes on policy terms and conditions
- Knowledge and skill set necessary to underwrite cyber-risk is extremely specialized
- Scope of coverage is highly specific to each cyber policy, with very little standardization across insurers

The Technical Perspective

- A moving target due to the evolving nature of cyber risk and uncertain claims environment
- Risk aggregation is a major concern due to IoT
  - Inter-connectivity increases the potential impact of cyber attacks due to the increased number of systemic risk points
- Developing models to asses the exposure is critical for pricing, underwriting, and ERM
  - Somehow needs to be accomplished with very limited data
- Can cyber-insurance step up to overcome these challenges?
  - There are concerns about the adequacy and utility of coverage in the event of a cyber-attack
- All this has limited insurers ability to more effectively penetrate this market

Market Profile

- Cyber risk insurance is the fastest growing P&C insurance segment
  - Estimated $3 billion in premiums in 2015 and anticipated to triple in four years
- Approximately 50 insurance carriers now offer some form of standalone cyber insurance coverage
- Offering cyber coverage as an endorsement to other traditional coverages is very common
- Larger companies more likely to purchase cyber insurance



Coverage Overview

Liability Coverage ('Third Party' Coverage)	
Privacy Liability	Liability costs associated with an inability to protect personally identifiable information, personal health information or a third party's corporate confidential information.
Network Security Liability	Liability costs associated with an inability to prevent a computer attack against your computer network or a third party's network.
Media Liability	Liability associated with disseminated content, including social media content.
Liability Mitigation Coverage	
Breach Response Costs	Direct costs expended to respond to a privacy incident. Costs typically include legal, public relations, notification, identity theft restoration, credit monitoring and forensic investigation expenses.

Coverage Overview

First Party Coverage	
Income Loss / Extra Expense	Income Loss / Extra Expense associated with a computer attack or system failure which disables your network.
Data Reconstruction	Costs to recreate, recollect data lost, stolen or corrupted due to an inability to prevent a computer attack against your network.
Extortion Costs	Costs expended to comply with a cyber extortion demand.
Regulatory Fines	Fines assessed by a federal, state, local or international regulatory body due to a data breach.

The Great Debate – Cyber Insurance vs Traditional Insurance

What if a cyber event leads to physical damage to property, as well as business interruption and other third-party liability exposures?

- **Should a cyber policy or commercial property policy cover such losses?**
- **Majority of cyber markets are reluctant to cover any bodily injury or damage to tangible property (and vice versa)**
  - Commercial property exclusion usually via CL 380 (LMA cyber attack exclusion)
- **Very polarizing topic, with varying views**
  - More coverage usually available under commercial property
  - Single cyber tower with an all-risk component to it reduces ambiguity?
  - Cyber extension to existing coverages across other lines would more effectively provide the coverage that's actually needed?
  - Where would the underwriting expertise need to sit?

Proposed Ideas to Mitigate Conundrum

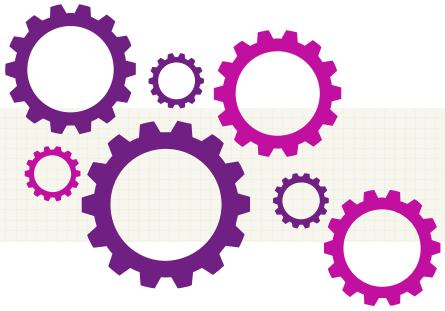
Public-Private Cyber-Catastrophe Reinsurance Scheme

"Insurers find writing cyber insurance difficult without reinsurers, but reinsurers need significant scale before the pooling effects make such reinsurance possible"

- **An addition or extension to existing schemes for terrorism**
  - Example: Pool Re in UK and TRIPRA in U.S.
- **Remove blockages that limit cyber insurance penetration**
  - Allays some of the concern around risk aggregation
- **Provides a way for businesses, insurers, and government to work together to manage cyber risk**
  - Encourages information sharing and insurance-based incentives for investment in cyber defenses

UK's Pool Re Scheme

- Not enough capacity in the insurance industry to cover the scale of potential losses that might arise from a cyber attack
  - Limited products available to insure against the risk of a cyber attack which businesses and infrastructure are exposed to
- Standalone Cyber Re vs expanding Pool Re?
- Immediate goal – not to get it perfect but to move one step closer to establishing a reinsurance scheme for cyber risk
- Support for state back cyber pool has been growing
  - Pool Re CEO Julian Enoizi publicly indicated that its structure could easily be adapted to address broader cyber risks



Advanced Cyber Risk Modeling

- Development of comprehensive cyber industry exposure database
  - Estimate potential financial losses to entire sectors and portfolios due to common vulnerabilities
- Analogous to catastrophe modeling done in the property insurance market for hurricane and earthquake risks
- Consider factors such as real-time security ratings of companies, exposure data, and supply chain information
- Both probabilistic and deterministic scenario modeling of (re)insured portfolio of cyber risk
- Scenarios used to gain a better understanding of potential aggregation risk from a large scale cyber attack
  - Example: cloud providers, payment processors, and blackouts

Other Ideas Proposed

- Holistic strategy with long-term relationship view
  - Insurers partnering with cyber security and/or technology firms
  - Including valuable services as part of the coverage, such as post-breach response coverage

Who's doing what?

Insurers

Vary in approach. Many insurers writing cyber have models for assessing individual insureds based on industry type, size, number of records and/or qualitative assessments of the insured's risk management procedures and risk culture.

Brokers

AON
Cyber Risk Diagnostic Tool "provides a high level understanding of the cyber risks facing an organization"

Marsh
Cyber IDEAL model "models probabilities and potential financial impacts of cyber events on individual organizations"

Willis Towers Watson
Cyber Quantified model for individual cyber risks and PRISM-Re model for insurer's cyber portfolio analysis: frequency / severity approach, full probabilistic models

CAT Modeling Firms

AIR
Stochastic modeling framework in development phase; working prototype

RIMS
Accumulation management tool based on 5 accumulation scenarios