Cyber Risk – Current State of the Market, Risk Modeling and Analytics

October 27, 2016

Willis Re

Cyber – opportunity or threat?

- Cyber represents fastest growing insurance market segment
- US market currently dominates but worldwide premium growth expected to increase dramatically
  - 2012 $1.3B (U.S. only) – Advisen
  - 2015 $2.4B (U.S. only) – Advisen
  - 2020 $7.5B (Worldwide) – PWC
  - 2025 $20B (Worldwide) – Allianz
- However, there is little available claims data to help determine cyber pricing and sources of exposure are evolving rapidly
- With greater interconnectivity of data, there is also a market fear about the scale of cyber accumulation exposure, although much of this is based on conjecture
- As in other lines, modelling would help inform underwriting decisions, free-up capacity and allow insurers to manage their accumulations with support from reinsurers
- There are few, if any, commercially available cyber underwriting models and Willis Re has been working hard to help clients better understand their exposures and fill the modelling "gap"

Increasing demand for cyber insurance from all sectors

What's driving it?

World's biggest Data Breaches

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

- Average cost per cyber crime: USA – USD 15.4M; GER –USD 7.5M; UK – USD 6.3M
- **52%** of all U.S. SME businesses were interested in buying Cyber insurance
- **41%** of all online adults have fallen victim to cyber attacks
- Top reason for US companies for not buying cyber insurance in 2015: **Low Limit**
- Major concerns are **loss of personal data** and **IP theft**

http://www.statista.com & Paper: CYBER RISKS:THE GROWING THREAT, Insurance Information Institute, 2014

Insurance and reinsurance market responses

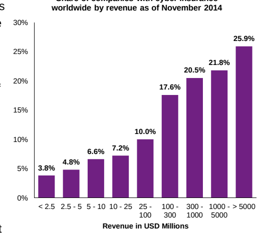
Insurance:

- Cyber insurance has its origins in the 1990's
- Currently one of the fastest growing insurance sectors
- Larger companies more likely to buy Cyber insurance
- Insurer product tailored to targeted market segments – i.e. Private, SME, Commercial Industrial
- Risk / retention appetite lower than for other classes
- Approx. 50 insurance carriers now offer some form of standalone Cyber insurance coverage
- Offering Cyber Insurance coverage as an endorsement to other traditional coverages is very common

Reinsurance:

- Cyber is often covered in PL reinsurance treaties
- Standalone treaties are typically QS or aggregate stop-loss
- Per Risk and Per Occurrence Excess of Loss present difficulties with definition of risk and occurrence

Share of companies with cyber insurance worldwide by revenue as of November 2014



Source:
Ponemon Institute; Hewlett-Packard - 2015 Cost of Cyber Crime Study

Cyber insurance: large potential but insurers are cautious

- The largest 5 providers of capacity have been the same 5 for the past 10 years – AIG, Beazley, Zurich, ACE/Chubb
  - AIG is considered the largest and is estimated to generate over USD100M in cyber-related premiums annually
- Current capacity for large financial institutions is $300M, but smaller insurers offer limits of $25,000 to a maximum of $5M to $25M
- Recent experience shows that corporations haven't bought enough insurance coverage to cover their losses:

(Amounts in $ millions)	Total Cost	Insurance Coverage	Net Loss to Company
Target Corp	252	90	162
Home Depot	63	30	33
Sony*	139	60	79
Anthem	> 100	100	???

**includes loss of cost recouped for leaked film*

- What's causing insurers to be so cautious in entering the cyber insurance market?

Risks and pitfalls exist

While opportunities are attractive, insurers need to consider risks and pitfalls

- 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
  - As a consequence of the limited historical claims, few precedents exist to handle potential coverage disputes on policy terms and conditions
- Risk aggregation and clash risk that comes from a potential attack remain as top concerns for insurers
- 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

All these have limited insurers' ability to effectively penetrate this market

Cyber Modeling and Analytics

Growth in cyber driving interest in quantification

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	MARSH	WILLIS TOWERS WATSON
Cyber Risk Diagnostic Tool "provides a high level understanding of the cyber risks facing an organization"	IDEAL "models probabilities and potential financial impacts of cyber events on individual organizations"; New GC / Symantec partnership to develop cyber cat model	CQ and NOQ models for individual cyber risks, PRISM-Re model for insurer's cyber portfolio analysis: frequency / severity approach, full probabilistic models

CAT MODELING FIRMS

AIR	RMS
Stochastic modeling framework in development phase with working prototype; one open-source scenario released with plans to release more	Accumulation management tool based on 5 accumulation scenarios x 3 severities

General framework of a cyber risk model

Hazard → **Exposure** → **Vulnerability** → **Financial**

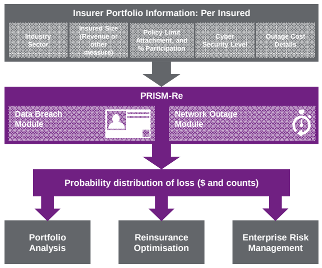
Hazard
- Source
  - Breach
  - Business interruption
  - Damage to assets
  - Extortion / theft
- Dynamics
  - Frequency
  - Severity

Exposure
- Value of digital assets
- Number of records stored
- Revenue
- Regulatory requirements

Vulnerability
- Size
- Industry
- Potential downtime
- Security protocols
- Other?

Financial
- Breach cost per record
- Lost revenue
- Damage to assets
- Insurance coverages offered
- Limits, sublimits, deductibles

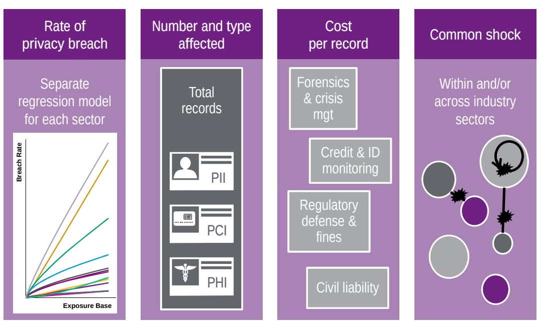
Modeling and risk appetite
PRISM-Re v2.0™



- PRISM-Re first released in 2015
  - Insurance industry's first cyber portfolio management tool
- 2016 release covers network outage as well as data breach
  - Two leading causes of cyber loss
- 2016 release covers losses worldwide
  - No longer just U.S. given cyber market growth implications
- Model has multiple applications
  - Accumulation control / downside risk estimation
  - Simulate cyber "contagion" risk within and between industry sectors
  - Monitor shifts in risk profile, guide improvements to portfolio composition
  - Help maintain risk adjusted pricing
  - Evaluate reinsurance strategies

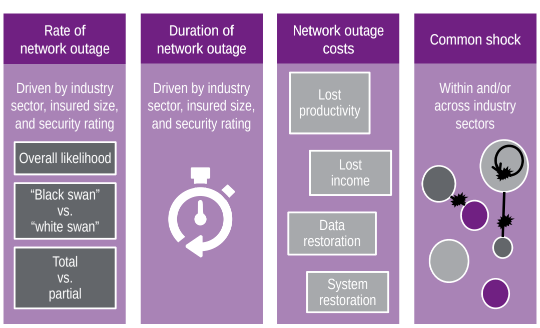
 CONFIDENTIAL

PRISM-Re mechanics: privacy breach module



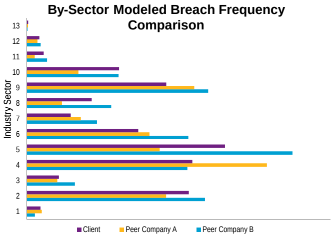
 CONFIDENTIAL

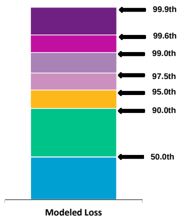
PRISM-Re mechanics: network outage module



 CONFIDENTIAL

Model application: benchmarking and contemplating downside





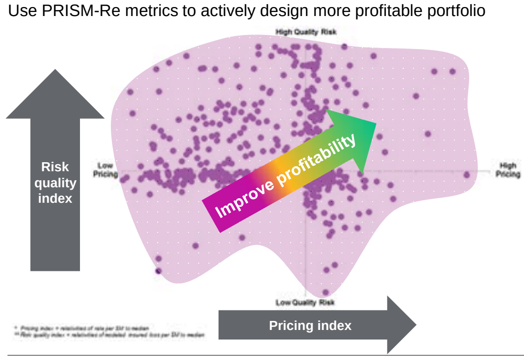
- Portfolio breach frequency by sector
- Benchmark against peer companies and industry

- Assessment of downside risk
- Assist with portfolio management and optimization, capital allocation, reinsurance decisions, etc.

 CONFIDENTIAL Willis Re 13

Model application: portfolio optimization

Use PRISM-Re metrics to actively design more profitable portfolio



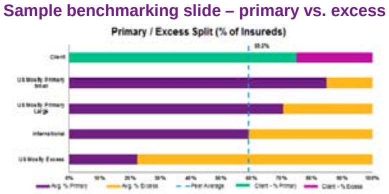
 CONFIDENTIAL Willis Re 14

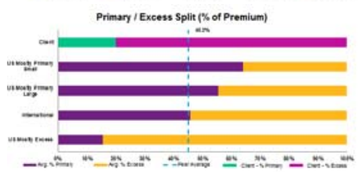
 Willis Re

Benchmarking overview

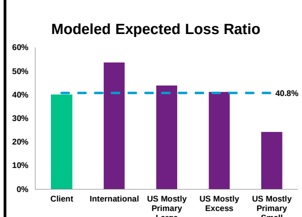
- Currently, there is no commercially available cyber exposure database for insurers to benchmark themselves against
- WTW's proprietary cyber database is constructed by consolidating actual cyber policies from clients/prospects
  - Robust dataset with over 7,500 cyber policies from a diverse mix of portfolios
  - Represents >$300M of annual GWP
- 4 cyber peer groups contemplated
  - International
  - US Mostly Excess (based on a 50% primary vs. excess threshold)
  - US Mostly Primary – Small (median revenue <$50M)
  - US Mostly Primary – Large (median revenue >$50M)
- Benchmark a company's cyber book against peer group averages to answer several frequently asked questions:
  - How does the portfolio's modeled ELR stack up against other cyber writers?
  - Is the portfolio's modeled volatility in line with peers?
  - Are they selectively writing the "good" (i.e. low expected frequency) risks in particular industry sectors?
- Provide more reinsurance-related peer statistics (e.g. CC, agg stop ROL, treaty capacity) to facilitate a discussion about cyber-specific reinsurance purchases

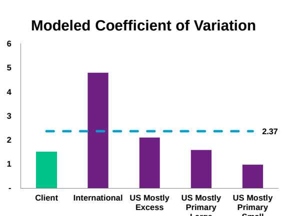
Sample benchmarking slide – primary vs. excess split





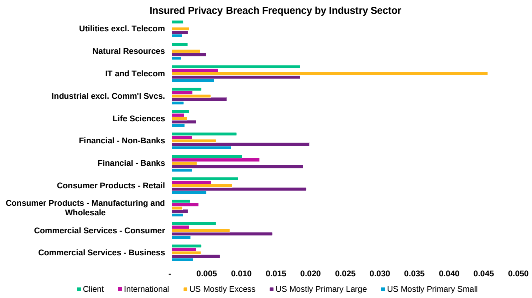
Sample benchmarking applications – modeled ELR & volatility





- Example client portfolio's modeled insured LR is in line with US Mostly Excess and its modeled CV is closest to US Mostly Primary - Large

Sample benchmarking applications – expected breach frequency



- Compare a client's modeled breach frequencies by sector against peer groups to make observations on risk selection

CONFIDENTIAL

Next steps in advanced cyber risk modeling

- Development of comprehensive cyber industry exposure database
  - Estimate potential financial losses to entire sectors and portfolios due to common vulnerabilities
  - 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
  - Analogous to catastrophe modeling done in the property insurance market for hurricane and earthquake risks
- Scenarios used to gain a better understanding of potential aggregation risk from a large-scale cyber attack
  - Example: cloud providers, payment processors, and blackouts
- 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

Willis Re Disclaimers