Lessons learnt from the unlikely marriage between Cyber security experts and actuaries in producing a practical approach to cyber modelling

Stavros Martis, KPMG
Ana Chavez, KPMG
Agenda

1. Overview of the Market
2. Cyber expert’s point of view and areas to consider
3. A practical modelling approach
Overview of the market
State of the London Market

- **Cyber Market continues grow**
  - It is clear that with new regulation such as GDPR that there is a need for cover beyond the US market.
  - According to The Betterley Report 2015, annual policy premiums are approaching $2.75 billion. It's widely acknowledged as the fastest growing class.
  - According to Allianz 2016 Risk Barometer, cyber incidents are considered the No. 1 emerging risk for the long-term future suggesting the client need is there too.

- **There is a need to differentiate in the market.**
  - Many of the larger players are exploring the incorporation of preventative services into their products (eg Pen Testing, Red Teaming, crisis Mgt.) The main challenge is innovating in this way without raising premiums.
  - The other way that insurers are differentiating is by offering higher limits. The most notable example being Munich Re & Beazley offering $100m limit (albeit with a large retention) in April 2016.

- **The other high profile topic within cyber insurance is silent coverage** across their existing products. A recent LMA exercise suggested this was most acute in Liability. Lloyd’s have issued scenarios to test syndicate exposures’ for silent cyber exposure.

- **We have seen a number of MGAs be prominent in this market** with Ryan Specialty Group, Scieumus and CFC.

- **Data is likely to be where future players will differentiate.**
  - Many players have looked for technology partnerships with IBM, Symantec, Bitsight etc. Others are building their claims taxonomy to build their own data assets to support with future pricing.
Underwriting and Claims

“Pre-Bind” Assistance on Underwriting

- Questionnaires/Interviews
- On-line assessments
- External penetration assessments (using third party vendors)
- Full reviews
- Or, just do nothing….
- Cost is a key consideration (average premium vs cost of pre-bind assessment)

Why should actuaries care? – If a pre-bind takes place, there could be more data to help with the parameterisation of the models. For example, you could start collecting scores from these assessments and start building relativities.

“Post-Bind” Value-Add Services

- These are additional services that the insurer can offer
  - Pen testing
  - Documentation and process reviews
  - Training
  - Incident response procedures

Again, if these happen, then claims experience should be better than if these do not take place.

On the claims front (incident response), different models are adopted

- Dedicated hotline
- Panel
- Hybrid

What is key here is the time to respond. The longer the response, the larger the ultimate claim cost
Scarcity of Data

- The London Market and Lloyd’s have spent a lot of time thinking about data capture.
- This is the obvious first step in creating stable and credible data in the long run.

Various initiatives:
- Lloyd’s
- Cambridge
- RMS
- AIR

- Commonality in collection of geographic information on insured companies using ISO country codes such as: US – United States, GB – United Kingdom etc.
- Standard Cyber Peril Codes, such as: PCY - Cyber security data and privacy breach & PCZ - Cyber security property damage
- Agreement on key indicators of cyber vulnerability such as: Enterprise Size as captured by revenue and headcount, Organization Industry or Business
- Aligned Cyber Coverages including, but not limited to:
  - Security Breach of Privacy
  - Liability
  - Business Interruption
  - Cyber Extortion
  - Replacement of Lost Data and Software
  - Regulatory fines
  - Physical Damage and Bodily Injury
- Common cyber risk attributes including: number and type of records held which could be breached.
- Identifiable Data Types at risk include but are not limited to:
  - Credit Card
  - PII (Personally Identifiable Information)
  - PHI (Personal Health Information)
  - IP (Intellectual Property)
- Identification of cloud service providers
- Internet Business Interruption potential
Coverage

- Variety of coverages and exclusions
- Package vs Standalone
- Affirmative vs Silent

<table>
<thead>
<tr>
<th>v1.0 Code</th>
<th>Cyber Coverage</th>
<th>% of Products Offering this Cover (Sample of 26)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Breach of privacy event</td>
<td>92%</td>
</tr>
<tr>
<td>2</td>
<td>Data and software loss</td>
<td>81%</td>
</tr>
<tr>
<td>6</td>
<td>Incident response costs</td>
<td>81%</td>
</tr>
<tr>
<td>15</td>
<td>Cyber extortion</td>
<td>73%</td>
</tr>
<tr>
<td>4</td>
<td>Business interruption</td>
<td>69%</td>
</tr>
<tr>
<td>12</td>
<td>Multi-media liabilities (defamation and disparagement)</td>
<td>65%</td>
</tr>
<tr>
<td>7</td>
<td>Regulatory and defense coverage</td>
<td>62%</td>
</tr>
<tr>
<td>14</td>
<td>Reputational damage</td>
<td>46%</td>
</tr>
<tr>
<td>3</td>
<td>Network service failure liabilities</td>
<td>42%</td>
</tr>
<tr>
<td>5</td>
<td>Contingent Business Interruption</td>
<td>33%</td>
</tr>
<tr>
<td>9</td>
<td>Liability – Technology Errors &amp; Omissions</td>
<td>27%</td>
</tr>
<tr>
<td>10</td>
<td>Liability – Professional Services Errors &amp; Omissions</td>
<td>23%</td>
</tr>
<tr>
<td>13</td>
<td>Financial theft &amp; fraud</td>
<td>23%</td>
</tr>
<tr>
<td>16</td>
<td>Intellectual property (IP) theft</td>
<td>23%</td>
</tr>
<tr>
<td>18</td>
<td>Physical asset damage</td>
<td>19%</td>
</tr>
<tr>
<td>19</td>
<td>Death and bodily injury</td>
<td>15%</td>
</tr>
<tr>
<td>-</td>
<td>Cyber terrorism</td>
<td>12%</td>
</tr>
<tr>
<td>11</td>
<td>Liability – Directors &amp; Officers</td>
<td>13%</td>
</tr>
<tr>
<td>8</td>
<td>Liability – Product and Operations</td>
<td>8%</td>
</tr>
<tr>
<td>17</td>
<td>Environmental damage</td>
<td>4%</td>
</tr>
</tbody>
</table>

Source: RMS
Data Issues

- We have spent the best part of the year trying to collate data from public other sources.
- There is information out there but there are pitfalls:
  - **Publications**
    - Inconsistencies between
      - Years (within the same publication)
      - Different reports
    - Definition of
      - Costs
      - “event” or “incident”
    - Population that contributed to the reports
      - Inconsistencies between years
      - USA vs everyone else
      - Sector differences
  - **Claims data**
    - Sparse
    - Have not observed large events yet
    - Companies are reluctant to publish
    - Sometimes, claims data include Tech PI claims
  
  - **Already Out of Date?**
Traditional Approaches may not work

- Cyber risk is a new risk, which does not lend itself to the use of traditional pricing and reserving approaches

**Limited Data**  **Uncertainty in contract wordings**

**Changing nature of the underlying threat**  **Silent vs Affirmative cyber**

**Impact**  

**Frequency**  **Severity**

An alternative approach:
- Drop down a couple of layers to look at cyber risk at the Sector/Country/Insured level
- Try to model the risk from ground-up, (starting from the technical characteristics of cyber)
- Talk to cyber experts!
Meeting the Cyber Security Expert....
Meeting the Cyber Security Expert….

• First date went badly…..

• At first glance, this marriage was doomed to fail…..
Meeting the Cyber Security Expert....

- Actuary’s view of the cyber experts:
  - Geeks
  - Very focused on the technical side
  - Whilst they do have access to data, they usually do not have a structured way of analysing this data
Meeting the Cyber Security Expert....

Actuary’s view of the cyber experts:

- Geeks
- Very focused on the technical side
- Whilst they do have access to data, they usually do not have a structured way of analysing this data

Cyber experts view of the Actuary:

- Geeks
- What on earth are they talking about?
- How can they possibly form views based on barely any data?
Cyber Expert’s Point of View
Dimensions to cyber risk

Threat Types:
- Who is likely to target your clients?

Geography:
- Which jurisdictions do they operate in?
- How good are they in preventing and detecting an attack?

Sector:
- What is their line of business?
Threat Types

Who would target you, your clients and why?

- **Organised crime** — Global, difficult to trace and prosecute
  - Motivation: Financial advantage
  - Impact to business: Financial loss

- **Competitors** — Competition or rivalry
  - Motivation: Gain business edge
  - Impact to business: IP theft, reputation damage

- **The insider** — Intentional or unintentional
  - Motivation: Grudge, financial gain
  - Impact to business: Distribution or destruction, theft of information, reputation loss

- **Hacktivism** — Hacking inspired by ideology
  - Motivation: Shifting allegiances – dynamic, unpredictable
  - Impact to business: Public distribution, reputation loss

- **State-sponsored** — Espionage and sabotage
  - Motivation: Political advantage, economic advantage, military advantage
  - Impact to business: Disruption or destruction, theft of information, reputational loss

Institute and Faculty of Actuaries
Geographic Distribution - Europe

Microsoft Security Intelligence Report 20
Malware encounter rates Q4 2015
Ransomware

Major growth in range of groups and tools since Oct 2015

44% of business hit in last 24 months
Most pay up

Small ransoms often only 1 bitcoin

Large scale extortion attacks

Particular threat to hospitals

4% of businesses hit in last 24 months
25% paid the ransom
42% of those got their data back
4% of individuals (61% in N.A.) hit
4% had a malware infection
25% paid the ransom
89% of those got their data back
Payment card attacks

EFTPOS remains a concern – although awareness has risen post Target

Card not present frauds are biggest growth area

But beware unlimited cash outs – banks can be a weak link

Roll-out of EMV (Chip and Pin) is helping – now US has shifted liability

Fraud levels remain stubbornly high (30-100bps) Complex liability model

TAILORED

Institute and Faculty of Actuaries
Broader industry attacks

Criminals now looking beyond financial sector
CEO and business email compromise fraud now rampant

FBI warn received fraud reports totalling $3.1 Billion
Recent example of $44 million fraud

Sophisticated social engineering
Networks of call centres

Attacks now tailored to firms, their business and their employees

LinkedIn
Persistent and targeted attacks

- SWIFT attacks followed
  - Attempted $951M fraud at Bank of Bangladesh

- Carbanak signalled a new type of attack
  - Persistent and stealthy

- $81M successfully transferred to Philippine casinos

- Other SWIFT attacks followed
  - Weak links?

- Speculation over criminal and State links and flow down of techniques

- Ukrainian Bank HACKED!
  - Hackers Steal $10 Million

HIGH END

Institute and Faculty of Actuaries
## Sector Characteristics

### Different attack patterns and severity profiles

- Utilities
- Transport
- Media & Telecommunications
- Arts & Entertainment
- Agriculture
- Non Profit
- Health
- Education
- Construction
- Manufacturing
- Mining
- Hospitality
- Retail
- Government
- Banking & Finance
- Defence
Return on Investment

- WHY BOTHER
- Front Running Attacks
- ATM Jackpot
- SWIFT Attack
- Making Money!

- Takedowns
  - 2 Factor Authentication
- Chip and Pin
- EFTPOS
- Ransomware
- Banking Trojans
- DDOS for extortion
- CEO Frauds

Cost to Criminal

- High
- Low

Income from Attacks

- $1 Low
- $10,000 Low
- $100 Million High
- $100 Million High

Institute and Faculty of Actuaries
The Threat Keeps Changing....
Modelling Approaches
A Variety of Approaches

- Bespoke quantitative and/or qualitative solutions (Primary Insurers/MGAs)

- “Cat models” to assist with accumulation/aggregation management
  - Brokers
    - AON
    - WTW
    - Marsh
  - Modelling Firms
    - AIR
    - RMS
KPMG Cyber Modelling Approach

- We work with clients to develop bespoke cyber models.
- Our key strength and focus is on the parameterisation of models (either for pricing or accumulation management purposes).

Stage 1: Construction of KPMG benchmark cyber model

Stage 2: Pricing of individual risks

Stage 3: Construction of aggregation model

Stage 4: Parameter Validation

Validation of Pricing & Accumulation models to ensure consistency in view of risk

Common inputs across all Models

- Cyber Intelligence
- Coverage details

- Exposure measurement & Forensic Input
  - Business Interruption
  - “Crown Jewels”

KPMG Insight: Benchmark Data, Threat Intelligence, Expert Judgement

KPMG’s Global Maturity Assessment Scoring Database

Company’s Cyber Insurance Framework

KPMG and Company Judgement

Benchmark Frequency & Severity
By Country, Sector, Company

Benchmark Frequency & severity adjusted for individual risks

Realistic Disaster Scenarios by Sector

Construction of Scenarios
Quantify Likelihood & Impact
KPMG Benchmark Cyber Model Output - Example

Define the Risk Segment
- Sector.
- Country.
- Company profile.

Determine the relevant threats for each Risk Segment
- DDoS.
- Ransomware.
- Extortion.
- Terrorism.
- Etc...

Frequency
- Annual probability of successful attack from available data/insights
- A% DDoS
- B% Malware
- C% Extortion

Adjust for:
- Forward Looking View of risk (Threat Intelligence Reports)
- Judgement
- Scoring (via KMPG’s Global Security Assessment Database)

Selected Parameters (annual probability of successful attack)
- X% DDoS
- Y% Malware
- Z% Extortion

Selected Variability
- +-%
- -%
- +-%
Define the Risk Segment
- Sector.
- Country.
- Company profile.

Determine the relevant threats for each Risk Segment
- DDoS.
- Ransomware.
- Extortion.
- Terrorism.
- Etc...

Severity
- Look at what the immediate effect is on the company
- Collect information that is a proxy for this effect

Create “model points” from each of the relevant threats to estimate costs split by heads of damage:
- Breach costs
- Fines
- Liability
- Etc...

Selected Parameters
- DDoS: $ $ $
- Malware: $ $
- Extortion: $ $ $

Selected Variability
- DDoS: +-%
- Malware: +-%
- Extortion: +-%
KPMG Benchmark Cyber Model Output – Example (Cont.)

Selected Parameters (annual probability of successful attack)
- X% DDoS
- Y% Malware
- Z% Extortion

Selected Variability
- +-%
- +-%
- +-%

Simulation

Individual Risk Pricing
Validation of reserving
IELRS
Capital Modelling
Example of Extreme Event Analysis

**Probability of Compromising general IT infrastructure**
This is based on market statistics and reflects the recorded successful attacks on the general IT infrastructure of a company.

**Rising Trend in attacks**
Increasing trend in attacks over the past 12-24 months. This factor allows for this trend to continue in the next 12 months, and derived using expert insight and experience.

**Probability of destructive attack**
This step is to reflect the fact that only a subset of the observed attacks relate to a malicious attack.

**Probability of Breaking into OT environment**
Attacks on the Operational Technology systems, which control key assets, are the most significant.

**Adjustment factor to allow for entry via other routes**
Attacks can also happen via third party vendors who act as subcontractors. This risk is increased if systems are centralised.

<table>
<thead>
<tr>
<th>Type of loss</th>
<th>Impact ($)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
<td>615</td>
</tr>
<tr>
<td>Loss of life</td>
<td>30</td>
</tr>
<tr>
<td>Repair costs and patches for IT and OT systems</td>
<td>5</td>
</tr>
<tr>
<td>Own company’s business interruption costs</td>
<td>13,850</td>
</tr>
<tr>
<td>Environmental impact plus third party business interruption</td>
<td>20,000</td>
</tr>
<tr>
<td>Clean-up costs</td>
<td>11,200</td>
</tr>
<tr>
<td>Regulatory fines</td>
<td>1,000</td>
</tr>
<tr>
<td>D&amp;O claims</td>
<td>5,000</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>51,700</strong></td>
</tr>
</tbody>
</table>
Conclusion
Conclusion

- Variety of underwriting approaches
- Data is an issue but there is a starting point
- Forming a forward looking view is key. Cyber threats are evolving fast.
- Different modelling approaches are being developed
- The insight from cyber security experts is available and we should embrace them
Expressions of individual views by members of the Institute and Faculty of Actuaries and its staff are encouraged.

The views expressed in this presentation are those of the presenter.