QUANTITYING CYBER INSURANCE’S GREAT ‘KNOWN UNKNOWN’

David Flandro
Global Head, Economic and Franchise Risk

Vienna, 5 April 2019
AGENDA

1. Evaluating cyber risk
2. The evolving state of Cyber cover
3. The response – unlocking the potential . . .
EVALUATING CYBER RISK
CYBER RISK LANDSCAPE

WHERE?

ONLINE
OFFLINE

WHY?

MALICIOUS
ACCIDENTAL

WHO?

EXTERNAL
INTERNAL

WHAT?

TECHNOLOGY
MEDIA
DATA
OVERVIEW OF CYBER THREATS AND RESPONSES

THE CHALLENGES

<table>
<thead>
<tr>
<th>Evolving...</th>
<th>Threats:</th>
<th>Vectors:</th>
<th>Targets:</th>
<th>Exposures:</th>
<th>Regulations:</th>
<th>Coverage:</th>
<th>Responses:</th>
</tr>
</thead>
</table>
|             | - Human actor: waves, targeted, game of cat and mouse  
- Increasing specialisation and division of labour, greater “collaboration” and sharing of expertise, copycat attacks | - Evolving attack types, e.g. social engineering, ransomware, DDoS attacks, cryptojacking, fileless malware, no-distribute tested multiscanned malware | - Targeted / non-targeted “splatter gun” approach  
- Industry by industry: retailers, financial institutions, healthcare providers, educational institutions, etc.  
- Services and service providers; eg. uptick in attacks on cloud services, ATM cashout attack, cryptocurrency exchanges | - Greater proliferation of small businesses  
- Greater penetration into certain industries; increased digitisation  
- Rising geographic diversity | - Regulatory changes: Lloyd’s / PRA, AM Best  
- Legislative changes, e.g. EU GDPR, US & Canada incl. California CPA, Singapore, HK, SK, Japan, China, Singapore, Aus, NZ PA etc. | - Significant growth from historic birth in tech E&O; continued evolution eg. IP theft, physical damage, bodily injury, personal lines etc. | - Could also consider changing levels of defence, mitigation, expertise, investment, education and a number of other factors that impact on the risk environment |
CYBER ACCUMULATION FRAMEWORK
SCENARIO EXAMPLES

- DDoS
- Zero day vulnerability
- Phishing

Subscenarios:
- Cloud network interruption
- Attack on payment processor
- DNS attack
- Ransomware
- Power grid outage
- Marine vessel collision
- Air traffic control attack
- Cloud data breach
<table>
<thead>
<tr>
<th><strong>Actor</strong></th>
<th><strong>Vector</strong></th>
<th><strong>Target(s)</strong></th>
<th><strong>Impact</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Level of sophistication, experience and collaboration</td>
<td>Zero day vs. &quot;patchable&quot; vulnerability</td>
<td>Use of AV filtering (known/unknown), IDS, firewall, monitoring</td>
<td>Robustness of incident response policy</td>
</tr>
<tr>
<td>Level of resources</td>
<td>Phishing vs exploit</td>
<td>Patching cadence and capabilities / sophistication of security team</td>
<td>Level of network segmentation / admin privileges policy</td>
</tr>
<tr>
<td>Motivations (ideological vs. financial) including cost vs. benefit</td>
<td>Targeted vs untargeted</td>
<td>Firmographic (# of employees, revenue band, industry, locations)</td>
<td>Data back-up frequency</td>
</tr>
<tr>
<td>Lead-in development time</td>
<td>Self-propagating potential (e.g. worms)</td>
<td>Self vs. third party hosted services and software</td>
<td>Proportion of business critical / revenue dependent systems impacted</td>
</tr>
<tr>
<td>Experience of recent successful or failed campaigns</td>
<td>Password and credentials policy / defaults unchanged</td>
<td>Security training for employees (e.g. Cyber Essentials)</td>
<td>Third party liability and downstream impact</td>
</tr>
<tr>
<td>Location / jurisdiction of actor</td>
<td>Network connected devices (Personal, IOT...) and associated security</td>
<td>Government contracts / desirable IP</td>
<td>Breach of Personal/Financial/IP Data</td>
</tr>
<tr>
<td></td>
<td>Single vs. multi-stage attack (worm -&gt; ransomware)</td>
<td>Number of endpoints</td>
<td>IT capabilities and resources</td>
</tr>
<tr>
<td></td>
<td>Physical Security</td>
<td>Previous breaches / infections</td>
<td>Security consultants and demand surge</td>
</tr>
<tr>
<td></td>
<td>Handling user submitted data</td>
<td></td>
<td>Presence of kill switch</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PR impact</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Potential trigger for another event</td>
</tr>
</tbody>
</table>
THE EVOLVING STATE OF CYBER COVER
GROWTH ESTIMATES OF GLOBAL CYBER INSURANCE PREMIUMS

Source: Guy Carpenter, Allianz Global Corporate & Specialty, Advisen, Association of British Insurers, Munich Re, PwC
Three key factors to drive growth of cyber market

1. High-profile losses and increased risk awareness, with a growing number of companies looking to their insurance carriers for effective and innovative risk transfer solutions to mitigate today’s and tomorrow’s risk landscape. Companies that do not have cyber insurance often cite cyber-related losses at other organisations as a trigger to purchase cover.

2. Greater regulatory security. Currently, around 90% of all cyber insurance products bought globally are thought to be purchased by American companies, due in large part to existing data protection regulations in the U.S. New laws in other jurisdictions which will make it compulsory for companies to report breaches to authorities and penalise them financially with fines for non-compliance, such as General Data Protection Regulation (GDPR) in Europe or the Privacy Amendment (Notifiable Data Breaches) Bill in Australia, are therefore likely to lead to considerably more demand over the next year or two, particularly outside the U.S.

3. Increased supply of insurance capacity, with an ever-growing number of insurers looking to enter the cyber market. This competitive environment is likely to see more favourable terms being offered to organisations over the next few years.
CYBER: PERIL OR POLICY?

FLUIDITY OF CYBER

Company A

- SPECIAL CRIME
- GENERAL LIABILITY
- PROPERTY
- E&O
- BOND
- CYBER COVERAGE
- WAR
- TERRORISM
CYBER: PERIL OR POLICY?

FLUIDITY OF CYBER

Company B

SPECIAL CRIME

GENERAL LIABILITY

PROPERTY

E&O

BOND

CYBER COVERAGE

TERRORISM

WAR
## CYBER ACCUMULATION FRAMEWORK
### KEY DATA FOR A CYBER POLICY (RISK AND AGGREGATION)

### Bare minimum
- Net limits (and coverage sub-limits), participations
- Inception and expiry dates
- Policy premium allocation
- Loss experience
- Waiting periods and deductibles
- Organisation size / revenue
- Industry sector

### Nice to haves
- Domain name
- Organisation name
- Country and location footprint
- Employee headcount
- Number of data records (PHI, PII, PCI)
- Data back up type
- Data back up frequency
- Parent type
- % Revenue by Internet
- Business interruption value per hour
- Retroactive date
- Key managed service providers

### Not generally captured and used… yet
- Network assessments
- Physical and system security
- Data segregation
- Remote access prevalence
- Data portability
- Risk management procedures
- Vendor management procedures
- Legal / regulatory policies
- Point of sales practices
- Healthcare data compliance
- Multimedia practices
- Presence of penetration testing
3 THE RESPONSE – UNLOCKING THE POTENTIAL . . .
CYBER MODELLING: THE RESPONSE
CREATING THE ‘DREAM TEAM’

Cyber analytics

Information security
- Cross-over: cyber risk vendor model assessment

Terrorism
- Cross-over: cyber-terrorism event analysis, shared tool development

Actuarial
- Cross-over: Experience and exposure rating, stochastic modelling

Catastrophe modelling
- Cross-over: Exposure management, tail-side model development

Strategic advisory
- Cross-over: regulator and rating agency advice, franchise value analysis
CYBER MODELLING: THE RESPONSE
OVERVIEW OF STRATEGY

Aggregation model development
- Eg. analytical, stochastic RDS tools
- Focus is on quantification of systemic events and associated uncertainty

Vendor model analysis
- Close working relationship with vendor modelling firms
- Continual assessment of aggregation tools and data schemas

Direct pricing tools
- Eg. primary cyber risk pricing tools, designed to assess appropriate cover for individual cyber risks

Data collection & analysis
- Focus on extension of data depositories; eg. historic breach information, exposure and claims benchmarking
• “Bottom-up” tool with a focus on systemic cyber BI & CBI dependencies in an insurer’s exposures

• Event type customisation by:
  – Service provider
  – Date
  – Event length
  – Market share
  – Locality

• Flexibility and transparency
  MetaRisk-style ‘clear box’
  – Reproducible calculation framework
    - Allows a number of different scenarios / service providers to be considered
  – Easy to use visual parameterisation selection stimulates discussion
The current vendor modelling landscape straddles a number of different characteristics…

- Underwriting Focus
- Insurance Industry Origin
- Tech Industry Origin
- Aggregation Focus
<table>
<thead>
<tr>
<th>Category</th>
<th>Vendors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk modelling</td>
<td>BitSight, Security Scorecard, FICO, Cyberwrite, Arceo, CyberCube, Corax, RMS, AIR, Cyence, Kovrr, Lloyd’s, Munich Re (proprietary)</td>
</tr>
<tr>
<td>Accumulation modelling</td>
<td>CyberCube, Corax, RMS, AIR, Cyence, Kovrr, Lloyd’s, Munich Re (proprietary)</td>
</tr>
<tr>
<td>Firmographic data</td>
<td>Clearbit, Crunchbase, Google, Dun and Bradstreet</td>
</tr>
<tr>
<td>Breach data</td>
<td>Risk Based Security, Advisen, Risk Based Security, Advisen, Verizon, PCS</td>
</tr>
<tr>
<td>Claims data</td>
<td>Ponemon Institute, Verizon, PCS **</td>
</tr>
</tbody>
</table>

* Summarised metrics only
** Claims > USD 20m
Cyence
- **Pros**
  - First cyber model
  - Some thought leadership
  - Extensive market presence
  - Collaboration with Lloyd’s and rating agencies
  - Some exploration of silent cyber
- **Cons**
  - Criticised for "black box" approach
  - Significant cost
  - Small number of scenarios

CyberCube
- **Pros**
  - Utilises Symantec “behind firewall” data
  - Leverage kill-chain scenario methodology
  - Expansive (and growing) scenario set
  - Some exploration of silent cyber
  - Benefits from Symantec security briefings
- **Cons**
  - Significant cost
  - Proprietary scenario synopses

Corax
- **Pros**
  - Raw data as well as modelling offered
  - Integrated risk and aggregation offering
  - Transparency of data and approach
  - Unique vector-based aggregation methodology
- **Cons**
  - Limited scenario set
  - Not yet considering silent cyber
  - Requirement for domain name info

Kovrr
- **Pros**
  - Some flexibility of offering
  - Some exploration of silent cyber
  - Focus on threat intelligence
  - Purports to have many scenarios
- **Cons**
  - Muted take-up rate
  - Less transparency of process

RMS
- **Pros**
  - Some thought leadership
  - Significant market presence
  - Strong database structure
  - Good exploration of silent cyber
  - Expansive scenario set
- **Cons**
  - Reliance on market share approach
  - Significant variation between versions
  - Model updates may not be included in package

AIR
- **Pros**
  - Some thought leadership
  - Extensive exposure Database
  - Transparency of methodology
- **Cons**
  - Limited focus on silent cyber
  - Muted take-up rate
  - Heavy reliance on technology partner for individual risk focus

Lloyd’s
- **Pros**
  - Freely available RDS specifications
  - Clear higher-level methodology
  - Widely used
  - Some ability to benchmark via market publications
- **Cons**
  - As non-Lloyd’s member, potentially limited access to core scenario parameters
  - Lacks nuance and granularity
  - Not probabilistic
Cyber model comparison: Cat Risk Management Conference, London, March 2019
• Inaugural comparison of five vendor models (RMS, CyberCube, Cyence, Corax, and KOVRR), the first time such an event has taken place
• Each vendor was given a consistent portfolio of approximately 50 organisations with standard insurance policy information to model
• Average Annual Losses and Aggregate Exceedance Probability Curves were shared on an anonymous basis

Observations:
• Data were a significant issue; very different revenue figures used by some of the vendors which was not controlled for in the outputs
• Results showed significant deviation across the board, including both AAL and AEP results
• Even in light of general variation, one significant outlier (well above the peer average)
• Multipliers of AAL to AEP showed (slightly) more consistency, indicating that view of risk is starting to show some convergence
• Although it raised as many questions as it answered, it is a key step moving forwards to better understand
Event modelling
• Vendor outputs, blends, or proxy

Large risk loss modelling
• Blend of experience and exposure methods

Attritional modelling
• Developed ULR analysis

Risk correlations
• Holistic representation

Stochastic engine
• Heightened loss clustering simulated

Simulated gross loss table
• Captured at risk, event, and aggregate level
Risk mitigation reduces upside potential, through cost of purchasing insurance cover.

Earnings given up = Economic cost of current insurance program

However, this also reduces downside risk significantly...

... and stabilises earnings by reducing its volatility

Risk Mitigation / Insurance Program

Cost of risk mitigation (at 200 year C.I.) = \frac{Earnings given up}{Reduction in downside risk}
FACETS OF OPTIMAL APPROACH
CVA MODEL: CREATING COVER

RISK PARAMETERS

- **Number of Records:** Year 1: $XXXM with X% YOY Change
- **Industry:** Healthcare/Financials/Industrials/Telecom Services etc.
- **Type of Company:** Public/Private/Govt
- **Number of Employees:** XXXX
- **Revenue:** Year 1: $XB with X% YOY Change
- **Security Level:** High/Med/Low
- **PCI Data:** Yes/No
- **Breach Response Plan:** Yes/No
- **BYOD Allowed:** Yes/No
- **Encryption Performed:** Yes/No
- **Discount Rate:** X%
- **YOY Premium Change:** X%

PARAMETERS AFFECTING FREQUENCY

- Main factors used to estimate the frequency parameter are:
  - **Revenue**
  - **Type of company**
  - **Interaction of sector and revenue factors**
  - **Interaction of type of company and revenue factors**
- Once the initial frequency parameter has been estimated, other factors used to calculate the final frequency parameter are:
  - **Security Level** – The higher the security level, the lower the frequency
  - **BYOD Allowed** – If BYOD is allowed, the frequency will decrease
  - **Encryption Performed** – If performed, the frequency will decrease

PARAMETERS AFFECTING SEVERITY

- Primary driving factor of the cost of a cyber event is the **number of records which have been breached**.
- Number of records is adjusted by the expert experience on the number of records usually breached in a cyber loss e.g. 9% of the time, around 90% to 100% of records are breached.

INSURANCE PROGRAMS ANALYSED

<table>
<thead>
<tr>
<th>Program</th>
<th>Limit</th>
<th>Retention</th>
<th>Estimated Year 1 Premium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program 1 (Current)</td>
<td>$10.0M</td>
<td>$750K</td>
<td>$250K</td>
</tr>
<tr>
<td>Program 2</td>
<td>$20.0M</td>
<td>$750K</td>
<td>$450K</td>
</tr>
<tr>
<td>Program 3</td>
<td>$30.0M</td>
<td>$750K</td>
<td>$600K</td>
</tr>
</tbody>
</table>
THERE IS VALUE IN A NUMBER OF DIFFERENT APPROACHES TO THIS PROBLEM!

CHALLENGES

- Moving “goalposts” e.g. exclusionary / affirmative wording, loss occurrence
- Lack of data: even less than for standalone polices! Although…
  - Experience of no claims not the same as no claims experience

POSSIBLE APPROACHES TO QUANTIFICATION

- Deterministic scenario based
- Premium loadings
- Tail-side extrapolation
- Probabilistic interpretations and combination of methodology

The key question… where do exposures lie?
SILENT CYBER
SILENT AGGREGATION MODEL DEVELOPMENT

Latest development is in the evaluation of systemic silent cyber risks accumulating across classes and insured entities

Version 1 expected by mid 2019

This is composed of a large event set which could pose a threat across multiple classes of insurance business. Customising to:

- Assess most material by industry
- Evaluate the potential for insured losses class by class
- Set up intuitive calculation framework for further analysis

Planned scenario dimensions:

- Class and subclass response evaluation
- Industry splits and scale / locality
- Specific cyber systems targeted
- Primary and secondary organisation impact

Example scenarios:

- Financial exchange hack
- Midstream energy infrastructure targeting
- National power grid outage
- Telecommunications network manipulation
- Manufacturing supply chain interruption
APPENDICES
# CYBER COVERAGE DETAILS FOR SELECT CLASSES OF BUSINESS AT LLOYD’S

<table>
<thead>
<tr>
<th>Class of Business</th>
<th>Exclusion Clauses</th>
<th>Coverage Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accident &amp; Health</td>
<td>None</td>
<td>Silent exposures in all policies.</td>
</tr>
<tr>
<td>Directors &amp; Officers</td>
<td>Cover given</td>
<td>Cover is likely to be available to insured directors for shareholder action and privacy action, subject to the usual policy exclusions for deliberate wrongdoing and insurability.</td>
</tr>
<tr>
<td>Environmental Liability</td>
<td>Yes</td>
<td>Silent exposures in some policies, although underwriters often attempt to exclude cyber when utilities risks are involved.</td>
</tr>
<tr>
<td>Financial Institutions</td>
<td>Cover given</td>
<td>Cover is being provided for Financial Institutions policies. There are also instances of electronic computer crime extensions being bolted on for free due to the current soft market conditions.</td>
</tr>
<tr>
<td>Fine Art &amp; Specie</td>
<td>None</td>
<td>Some cover is being provided for risk of theft from a cyber attack.</td>
</tr>
<tr>
<td>General Liability</td>
<td>None</td>
<td>Silent exposures in all policies. A General Liability policy has already paid out a loss of this type in the US.</td>
</tr>
<tr>
<td>Marine Cargo</td>
<td>CL 380 – excluded unless endorsed for war</td>
<td>Exclusions are often amended to allow for cyber cover.</td>
</tr>
<tr>
<td>Marine Energy</td>
<td>CL 380 – excluded unless endorsed for war</td>
<td>Some uncertainty over whether exclusions are watertight.</td>
</tr>
<tr>
<td>Marine Hull</td>
<td>CL 380 – excluded unless endorsed for war</td>
<td>Silent exposures in some policies (for example, risks such as small and pleasure crafts).</td>
</tr>
<tr>
<td>Professional Indemnity</td>
<td>Cover given</td>
<td>Cover is often available for litigation and investigation costs, although the insurability of any fine or penalty arising out of the investigation is questionable. Cover for the Data Subject Access Request process is unlikely to be available.</td>
</tr>
<tr>
<td>Property Damage &amp; Business Interruption</td>
<td>Typically excluded NMA 2914 &amp; NMA 2915</td>
<td>Most PDBI policies exclude losses that arise from electronic data. Property policies cannot cover non-tangible assets by law. Policies can only respond if there is a direct physical loss or damage to the insured property.</td>
</tr>
<tr>
<td>Space</td>
<td>None</td>
<td>Silent exposures in most policies, although there is some disagreement on the cover provided. Some underwriters are attempting to bolt on cyber, but insureds are pushing back in these instances, saying it is already covered.</td>
</tr>
<tr>
<td>Terrorism</td>
<td>Typically excluded NMA 2914, NMA 2915 &amp; CL 380</td>
<td>Standard terrorism policies typically exclude physical losses or damage caused by ‘attacks by electronic means’. Some underwriters have watered down exclusions to write-back physical damage in the event of a cyber terror event.</td>
</tr>
</tbody>
</table>
**GC APPROACH**

**CYBERCUBE**

1. **Historic loss data**
   - Claims data
   - Development partner data
   - Expert insights from research

2. **External security data**
   - Specific company perimeter data
   - Threat telemetry
   - Vulnerability info
   - Web servers banners & end of life products

3. **Internal security data**
   - Web attacks
   - Targeted systems
   - Tactics, techniques & procedures (TTPs)
   - Infection rates
   - Powered by Symantec

4. **Enterprise data**
   - 7M+ companies
   - 50% USA
   - Industry Segments
   - 15% – 30% SME
   - Business financial & cyber dependencies
Data Schema
User-friendly data schema allows user to enter information on underlying insureds and (re)insurance terms and conditions
Partial data: learning algorithm utilises EIL/microsegment information to augment user input
3 mandatory insured company fields: Country | Sector | Revenue Band
9 mandatory insurance contract fields

Scenario analysis
Metrics: Conditional loss | Annual probability | Average Annual Loss Contribution
Drivers of loss: Clients | Sectors | Geography | Company Size

Probabilistic analysis
Adjustable parameters for stochastic analysis
Outputs: scenario contribution | measures of uncertainty | year loss tables

GC APPROACH
CYBERCUBE
CONTACT

David Flandro
Global Head,
Economics and Franchise Risk | Guy Carpenter
+44 (0) 20 7466 1311 | +44 (0) 7775 757 979
david.flandro@jltre.com