CSP WORKSHOP
CYBER INSURANCE FROM A BROKER’S PERSPECTIVE

27 April 2015

Stephen Wares
Cyber Risk Practice Leader — EMEA
London (Tower Place)
## Insurance Communication Gap

<table>
<thead>
<tr>
<th>Description</th>
<th>Source</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage of CEOs or CIOs of large organisations who believe they have insurance that would cover them in the event of a breach.</td>
<td>Information Security Breaches Survey 2014, Department for Business, Innovation &amp; Skills (BIS).</td>
<td>52%</td>
</tr>
<tr>
<td>Percentage of CROs or CFOs who state that their organisation has bought cyber insurance.</td>
<td>Marsh and Zurich cyber risk surveys.</td>
<td>15%-20%</td>
</tr>
<tr>
<td>Percentage of firms with cyber cover, whether as standalone cover or implicit in other policies.</td>
<td>Marsh and Zurich cyber risk surveys.</td>
<td>10%</td>
</tr>
<tr>
<td>Actual penetration of standalone cyber insurance products among UK large businesses.</td>
<td>Estimate based on policies placed/written by insurer project participant.</td>
<td>2%</td>
</tr>
</tbody>
</table>
Taxonomy of Cyber Risk for Corporations

1. A Malicious Attacks
   - **Actors**
     - State sponsored
     - Terrorists
     - Private enterprises
     - Cyber criminals
     - Activists
     - Current/former Employees
     - Lone actors
   - **Capability/Attack Sophistication**
     - From commodity tools to bespoke attacks driven by cyber experts
   - **Persistency**
     - Short-term/opportunistic
     - Automated/untargeted scans
     - Long term and persistent threats
   - **Proximity of the Attacker**
     - Internet/remote external attack
     - Local network external attack (e.g. WIFI)
     - Insider attack with network access
     - Physical access to IT equipment (inc. by subversion of employees)

2. Point of Attack/Failure
   - Within the organisation
     - The individual
     - The device
     - The system
     - The information
     - The network
   - External to the organisation
     - IT/infrastructure providers
     - Non IT supply chain/partners

3. Damage
   - **Type of Damage to Companies**
     - Theft of IP/commercially sensitive information
     - Business disruption/interruption
     - Data and software deletion/destruction
     - Direct financial loss
       - Theft of funds
       - Extortion payments
     - Third party liabilities (customers, employees, shareholders actions) and regulatory actions
       - Disclosure of third party data
       - Other
     - Reputational loss
     - Physical damage
       - People
       - Physical assets
     - Investigation/response costs
   - **Other Damaged Parties**
     - Supply chain companies
     - Employees
     - Private customers/Public

* Actors often correlated with MOTIVATION (1 Warfare/terrorism, 2 Propaganda, 3 Commercial gain/advantage, 4 Direct financial gain, 5 Protest, 6 Fun/demonstrate ability, 7 Revenge)
Existing Solution to the Cyber Coverage Maze

Brokers to provide businesses with a **statement of cyber assurance**, based on a review of exposure and cover versus risk appetite. The key elements of this approach are:

- **Identification of relevant cyber perils**: Based either on client scenarios generated in-house or pro-forma scenarios adapted to the client, which reflect those relevant for the firm’s industry and profile.

- **Cyber gap analysis**: Determine the extent of cover provided in the event of a cyber incident, including traditional policies’ response to a cyber event and the response of specific cyber cover that is in place.

- **Identification of solutions for uninsured risks**: Identify and arrange the appropriate cover to address uninsured risks where an insurance solution is available.

- **Cyber assurance**: Formal report, including assurance statement that cyber cover is in place to an agreed specification for those insurable risks that have been identified, and as appropriate to the firm’s risk appetite.
Pricing Maturity

Relative pricing index, property = 100
Based on Rate on Line for primary layer for companies with turnover < US$1 billion

## Building an Underwriting Submission

<table>
<thead>
<tr>
<th>Underwriting information</th>
<th><strong>Network information</strong></th>
<th>Outsourcing and third parties</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Backup</strong></td>
<td></td>
<td>Resilience and recovery</td>
</tr>
<tr>
<td><strong>Physical security</strong></td>
<td></td>
<td>Training and staff</td>
</tr>
<tr>
<td><strong>Policies</strong></td>
<td></td>
<td>IT security tools</td>
</tr>
<tr>
<td><strong>IT security process</strong></td>
<td></td>
<td>Updates and patching</td>
</tr>
<tr>
<td><strong>Legal requirements</strong></td>
<td></td>
<td>Data security</td>
</tr>
<tr>
<td><strong>PCI compliance</strong></td>
<td></td>
<td>Data management</td>
</tr>
<tr>
<td><strong>Records numbers and type</strong></td>
<td></td>
<td>Content</td>
</tr>
</tbody>
</table>
What (or Who) Is Insured?

Owned

Outsourced
The Elephant in the Room

Aggregation
# Aggregation and (Re)insurance Capacity

<table>
<thead>
<tr>
<th>Description</th>
<th>Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global exposure of the insurance industry to cyber risk total value.</td>
<td>GBP100 billion.</td>
</tr>
<tr>
<td>Maximum global (re)insurance capacity any “one event” for natural catastrophe (Tokyo or Californian earthquakes).</td>
<td>GBP65 billion.</td>
</tr>
<tr>
<td>Maximum global insurance/reinsurance capacity for a nuclear first-party loss (more comparable to cyber).</td>
<td>GBP3 billion.</td>
</tr>
<tr>
<td>Range of possible maximum loss (PML)/total exposure ratios for property portfolios.</td>
<td>0.15% (for UK property) — 20% (PML for hurricane for small exposed Caribbean island).</td>
</tr>
<tr>
<td>PML for cyber (assume the same PML/total exposure ratio of selected property portfolios).</td>
<td>GBP150 million — GBP20 billion.</td>
</tr>
</tbody>
</table>
Further Reading

- www.uk.marsh.com

Conclusion

- Organisations should ensure that their cyber risk is fully investigated and understood.

- Insurance positions as they relate to cyber risk should be investigated and accurately communicated within the organisation.

- The insurance industry currently has a huge appetite for insuring cyber exposure, but market growth will create some challenges and changes.

- Better modelling tools are required by the insurance industry to ensure that insurers are underwriting within capacity constraints.

- Insuring cyber exposures is complex and fractured across many policies. Organisations need to make full use of the expertise that exists within their broker to get the right outcomes.