Aon Risk Solutions
Global Risk Consulting | Captive & Insurance Management

Cyber risk and the captive market - a match made in the cloud?

With increasing news coverage of cyber-attacks and despite indications of interest, *Aon's 2014 Captive Benchmarking Study* confirms that only 1% of captive owners are funding cyber risk through their captives. A surprising result which has prompted us to further investigate the possible reasons why, especially since prior Aon research suggests much higher interest levels.

The associated costs of cyber threats are increasing for entities in every industry sector. The legal exposure, reputational harm and business interruptions that may result can wreak havoc on a company's bottom line. This was made clear in *Aon's 2014 Underrated Threats Report,* where 83% of respondents (Captive Directors) felt that the ranking of #18 in *Aon's Global Risk Management Survey 2013* for cyber risks (computer crimes/hacking /viruses/malicious codes) was severely underrated, a finding that was consistent along regional and revenue categories.

In *Aon's Global Risk Management Survey 2013*, 7% of respondents (Captive Owners) indicated interest in underwriting cyber risk in a captive over the subsequent five years. Most cited the lack of appropriate cover in the commercial market place as the reason.

However, in *Aon's 2014 Captive Benchmarking Tool*, which captured data from over 1,000 Aon managed captive clients, the number of captives writing cyber currently, is reported at 1%, a number which has remained static since 2012.

The reluctance for many organisations appears to derive from the challenge of gaining an estimation of the cyber risk exposure and quantification of consequences of cyber events, a challenge equally reflected in the reluctance of organisations to purchase cyber insurance from the insurance market.

Current situation

As mentioned earlier, only 1% of captive owners, according to our benchmarking study, are funding cyber risk through their captives. For such a large and looming potential source of liability this is a remarkably low number.

When analysing those captives that are writing cyber risk, it is no surprise that the majority are from the US healthcare industry. This development reflects the importance of healthcare companies providing protection due to the implementation of the Patient Protection and Affordable Care Act (commonly called the Affordable Care Act or 'Obamacare') in the United States which places an obligation on the medical company and particularly hospitals to have electronic medical records which of course would be open to cyber-attack.

Other industries that feature are professional services groups, financial institutions and retailers which we believe will become more prominent as the reliance on online tools for such industries continues to grow.

For EU based captives, proposed EU legislation has also stoked interest. The legislation will empower national data commissioners to fine companies that violate EU data protection rules and could lead to penalties of up to €100 million or up to 5% of the global annual turnover of a company - a significant reason to be on top of managing your data security risks. In addition to cyber security regulatory change, the regulatory landscape of the European Insurance regime has also prompted interest as the risk-based capital model of the Solvency II directive promotes the diversification benefits of writing new and additional insurance covers.

The chosen policy limits are quite interesting and appear to reflect the relatively unknown quantity of cyber insurance and captive placement. The variance is large (anywhere from $50k per occurrence to $50m per occurrence) and most captive cyber limits are based on what the market insurers are offering, both in terms of cover and pricing. At this point, few organisations understand their individual exposure to a level that would allow a scientific approach to calculating the organisation's cyber exposure. This is perhaps also reflected in the fact that almost all captives writing cyber are issuing 'standard' policy wordings, i.e. derived from the insurance market, rather than utilising a bespoke policy wording in line with the organisation's particular exposures and indeed the gaps in cover not provided by other insurance policies (Professional Indemnity, Business Interruption, General Liability, Commercial Crime, etc.). Again, this suggests that clarity about cyber exposure is not yet at a mature level of understanding.

There is an indication that captive owners that do write cyber do so out of a desire to better understand their cyber exposure rather than doing so as a reaction to an unresponsive insurance market.

Cyber liability is sometimes perceived not to be material enough to justify inclusion within the captive alongside the traditional covers of liability and property, yet when companies examine the value of their intangible assets as compared to their tangible assets, they begin to draw different conclusions. Perception of low cyber risk is also sometimes informed by the fact that "off the shelf" insurance market cyber offerings lack consistency.

The findings identify that a challenge remains for corporates to gain a clearer understanding of the specific cyber risk scenarios faced by their company and a better quantification of the consequences of these potential risks in order to make an informed decision on whether to write cyber insurance in their captive.

Responding to the challenges – how can a captive assist?

Bespoke solutions

Where an external market is unresponsive to any particular cyber risk needs, the opportunity exists to develop specific cyber policies using a captive. This flexibility could facilitate cover that would encompass highly correlated risks, for example cyber and reputation, which may not be packaged in the commercial market. Additionally, in the first year given the greater risk maturity of reputational risk, it would also be possible to access the reinsurance market and facilitate a more efficient transfer of risk. The cyber reinsurance market, accessible through a captive, currently offers significantly greater capacity than the primary insurance market and is particularly relevant for the catastrophe type exposures.

We also see the use of a captive giving flexibility in designing an optimal cyber risk transfer structure. Where adequate cyber first party loss, third party liability and crisis expenses cover may be available in the reinsurance market, the captive provides the ability to retain the special cyber risk covers not so readily available in the market, for example:

- Future lost revenue
- Dependent system failure business interruption
- Physical damage or bodily injury resulting from cyber peril (excess/DIC above other applicable insurance)
- First-party loss of inventory due to technology failure
- Loss of value of intangible assets

Where the premium is less material, a cell captive (within a Protected Cell Company 'PCC') could support the same objective of programme flexibility especially when it comes to the potential ring-fencing of a new risk or a desire to keep a new risk such as cyber liability separate from those in a captive.

Risk incubation

As with other 'non-traditional' risks, the captive can act as a 'risk incubator' for cyber risk thus recording the data/information about the risk currently unknown both within the organisation and the insurance market. Theoretically this data, over time, can empower the understanding of the cyber exposure hence allowing informed decision making in the risk financing decision process. However, this process does not happen automatically and where claims are not arising, little will be learned; hence a more focused effort, the correct approach and resources are required. While the inclusion of cyber insurance in the captive programme can promote a greater risk management focus as part of the captive oversight, it will likely need a much more concerted process to more accurately quantify the true cyber exposure.

This is perhaps where the recycling of profits being made within the captive can be utilised to fund the necessary time and expertise particularly in the area of quantification. This re-investment of results from self-insurance/captive can be both investigatory as well as ongoing in terms of cyber risk management initiatives, managing down the risk of exposure on a continuous basis. So, how would such a self-funded 'bursary' be utilised in order to achieve 'Cyber clarity'?

Captive investment in the Cyber Clarity process

What can go wrong and what could be the financial impact?

The first step to assess a company's cyber exposure should include an overview of the digital assets and a list of threats. Of vital importance is a cyber-risk assessment workshop with key stakeholders, to identify the cyber risk scenarios, followed by an assessment of the direct consequences (i.e. financial loss, destruction of digital assets or business interruption), an assessment of the indirect consequences (i.e. reputational damage, errors & omissions claim or loss of customers) followed by quantification of both.

This should be followed by running the input and scenarios through a cyber cost framework, which also factors in publicly and non-publicly available information about actual cyber losses, ultimately providing the organisation with an estimated maximum loss and most likely loss values for each selected scenario. This in turn should allow the company to provide a high-level estimation of holes in coverage or losses which will give a subsequent quantitative assessment of business interruption from cyber.

How is my company protected?

A key aspect of protecting a company against cyber risks is of course being sufficiently able to manage the risks where possible. Each company should assess their cyber risk management capabilities (firewalls, system operational procedures) and ideally benchmark these standards against industry and risk-appropriate standards including but not limited to ISO 27000 and the National Institute of Standards and Technology ('NIST') frameworks.

This information regarding IT and process controls can be used for two key purposes:

1. We can adjust the quantification modelling to account for the way risk mitigation techniques reduce the probability of certain scenarios
2. We can build a roadmap for the organisation to increase the level of cyber risk maturity with specific recommendations, allowing the information security team to clearly outline the return on investment for additional security measures

Will my insurance respond?

Following the identification of potential threat scenarios the company should then analyse the insurability of these threats through a series of stress tests, analysing each of these cyber risk scenarios against their current insurance portfolio. The results of this output can empower the adjustment of the scope and limit of current insurance policies and to make a data-driven decision about purchasing a cyber insurance policy or indeed placing such a policy in its own captive.

Following this process, the organisation can be equipped with a powerful, data-supported roadmap to assist and advise management decisions about risk mitigation/transfer/retention and insurance.

Conclusion

Cyber liability is a growing issue for organisations globally and it is no longer acceptable to turn a blind eye or be ill-prepared for a potential large loss. The low level of cyber in captives appears to align with a lack of clarity of the cyber risk exposure and quantification of consequences of cyber events, a challenge equally reflected in the reluctance of organisations to purchase cyber insurance from the insurance market. It is clear that the insurance markets also have more to do to understand cyber risk and offer insurance policies that will provide the correct protection. However, only the ability of an organisation to articulate their own risk profile to support better submissions to underwriters can truly drive this objective. A captive does not provide all of the answers but does offer a focal point to gain clarity of this risk, with the strengthened claims and exposure data and market knowledge enabling the implementation of an optimum cyber risk transfer structure.

To learn more about Aon's Cyber capabilities, please visit our Cyber Risk website at www.aon.com/risk-services/cyber.jsp. In addition, we invite you to complete our free Cyber Diagnostic Tool , by going to www.aoncyberdiagnostic.com. This will help quantify and benchmark your Network Security and Privacy exposures. The questionnaire only takes 10 minutes to complete and you will receive a tailored risk benchmarking report.

Contact us

John English
Regional Managing Director, EMEA
t +44 (0)20 7086 3040
john.english@aon.co.uk

Fernando Caballero de la Sen
Director
t +34 91 340 5096
fernando.caballero@aon.es

About Aon

Aon plc (NYSE:AON) is the leading global provider of risk management, insurance and reinsurance brokerage, and human resources solutions and outsourcing services. Through its more than 66,000 colleagues worldwide, Aon unites to empower results for clients in over 120 countries via innovative and effective risk and people solutions and through industry-leading global resources and technical expertise. Aon has been named repeatedly as the world's best broker, best insurance intermediary, best reinsurance intermediary, best captives manager, and best employee benefits consulting firm by multiple industry sources. Visit aon.com for more information on Aon and aon.com/manchesterunited to learn about Aon's global partnership with Manchester United.

Visit aon.com for more information about Aon.

Aon
8 Devonshire Square
London EC2M 4PL
United Kingdom