Cyber Insurance Market Update

Overview

- The market is still in its infancy, and penetration rates for standalone cover remain low in Australia
- Australia's mandatory data breach notification laws take effect 22 February 2018; those in the EU commence three months later, potentially further impacting some Australian businesses
- At minimum, organisations should be developing data breach response plans
- The Enterprise Internet of Things, and the increasing use of the cloud for data, further increase the need for boards to focus on cyber risk exposures

State of the market

While cyber is evolving at a rapid pace, there continues to be a much smaller uptake in cyber insurance across all levels of corporates in Australia, than is the case in the US. The EU is somewhere in the middle, although they are also becoming increasingly concerned about their new mandatory breach notification laws.

Nevertheless, cyber insurance is on a fast moving upwards trajectory and has been growing at levels not previously seen in traditional lines of business. The global standalone cyber insurance market, estimated at around $2bn–$3bn in premiums today, could reach $20bn by 2025, according to Allianz.[1]

We have seen a consistent trend of increasing capacity and capabilities in the local cyber market over the last 36 months. Policy coverage has markedly improved with insurers changing focus from a pure reimbursement policy to providing an immediate triage solution.

The local market is now able to deliver upwards of $150m in capacity with almost all major insurers now participating. Recent market entrants/newly released wordings include the likes of XLCatlin, HDI, Swiss Re and QBE.

Rates continue to be competitive, in part driven by more market entrants; however the expectation is that they are approaching minimum premiums levels.

Although Insureds are focusing on improved risk management around cyber exposures, such improvements may not necessarily correlate with a proportional reduction in premiums or improved cover. In part this is due to insurers already heavily discounting premiums in order to secure placements, and coverage is already significantly improved compared to last year.

Whilst the breadth of coverage has increased, it should be recognised that insurers' policy wordings are still written on more traditional formats, and will require enhancements to certain terms and conditions to provide clarity of coverage and peace of mind for the insured.

Data breach: it's about to get serious

Australia's mandatory data breach notification laws come into effect from 22 February 2018. They apply to public and private organisations that are already subject to the Privacy Act, which includes Australian Government agencies (excluding state and local government) and all businesses and not-for-profit organisations with an annual turnover more than $3 million.

It's clear that a significant data breach could be financially crippling for many organisations. The penalties for "serious or repeated non-compliance with mandatory notification requirements" include fines of up to $360,000 for individuals and $1.8 million for organisations.

Additional resultant costs could range from business interruption, incident response, third party claims and legal costs, to customer notification expenses and damage to data. Reputational costs and the possible loss of confidence from shareholders and other stakeholders add to the impact of such an event.

1. www.agcs.allianz.com/insights/expert-risk-articles/cyber-risk-2025/

AON
Empower Results®

In the US, where there have been many prominent data breaches, class actions have been taken against directors and officers of hacked organisations.

What is your exposure, how will you respond?

Over the past 12 months we have been assisting clients with risk quantification exercises to identify the scope of their potential cyber issues, and then working with insurers to develop policies to address possible exposures. Many such policies also provide access to incidence response panels that bring together experts in fields such as forensics, technology, legal, credit monitoring, PR and more.

In preparing for the mandatory breach reporting environment, organisations should now be developing response plans to answer questions such as:

- The actions to be taken if a breach is suspected
- Who is responsible for each of these actions
- Who will provide the specialist expertise, not currently available in house

The website of the Office of the Australian Information Commissioner (www.oaic.gov.au) contains a comprehensive guide to developing a data breach response plan.

EU laws also set for 2018

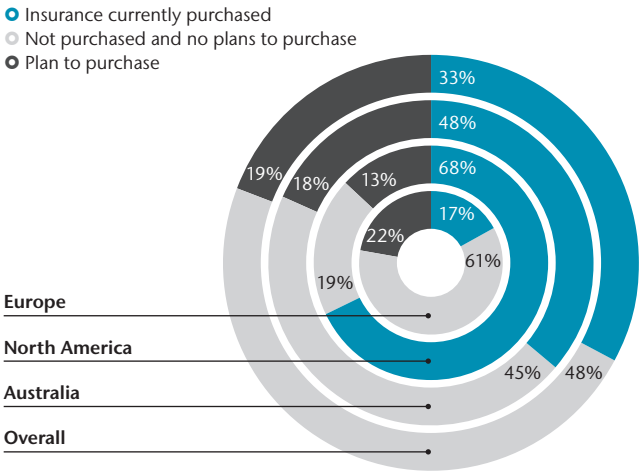
The EU's new General Data Protection Regulation (GDPR) will come into force in the first half of 2018. Australian businesses with EU-based customers will also be subject to the provisions of these regulations, which are more stringent and onerous than ours. For example, while the Australian legislation gives businesses 30 days to notify, the EU notification deadline is 72 hours, with fines that can scale up to as much as 4% of an organisation's global revenue.

In a connected world where business transcends geographic boundaries, every aspect of cyber risk needs to be a key boardroom concern.

Australian business remains underprepared

Although the Australian responses to Aon's 2017 Global Risk Management Survey show that cyber has risen to be a top-five risk concern locally, Australian business remains largely underprepared and complacent.

Cyber Purchasing Patterns



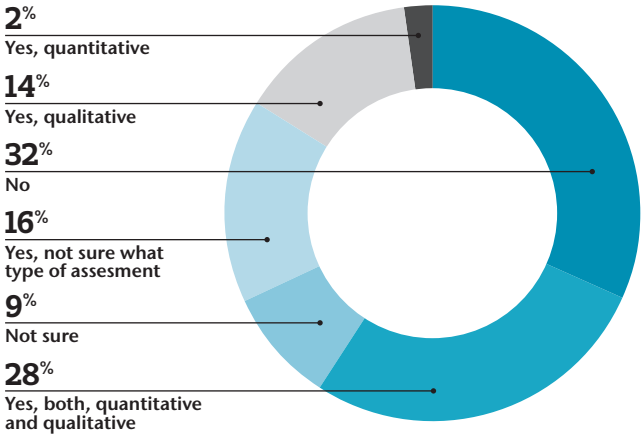
Source: Aon Global Risk Management Survey 2017.

There remains a perception among larger organisations that their systems and protocols are okay, and that their IT people are across all relevant issues. Yet, not only have some of the world's largest companies fallen victim to malicious cyberattacks, so too has the US National Security Agency (NSA) — the very people that possess all the security tools in the toy box.

From smaller organisations we hear the sentiment, "we're too small; we're not a target", while in reality they are simply softer targets.

AON
Empower Results®

Cyber Risk – Completed Assessment



Source: Aon Global Risk Management Survey 2017. Australian results.

Vulnerabilities attract organised crime

While hacking was once mainly a pastime for computer geeks, the recent WannaCry and Petya ransomware attacks demonstrate the increasing involvement of organised crime in cyberattacks. They also highlight how a lack of formal cyber security processes and protocols are leaving organisations unnecessarily vulnerable to such attacks. Common shortcomings include:

- Inadequate employee education and enforcement of corporate cyber security policies
- Failure to update operating systems or apply security patches
- Lack of a process for scanning inbound emails with a dedicated security product
- Continued use of outdated operating systems to run legacy applications that can't be patched.

At the same time, every new technology connected to an organisation's network, has the potential to open another attack vector for malicious actors looking to steal that company's IP or customer data, hold it to ransom, or even bring that business to its knees.

Looking ahead

As new technology is developed and adopted, the scope of cyber risk continues to grow and evolve.

The introduction of mandatory data breach notification laws in Australia, the EU and elsewhere will continue to see a rise in the uptake of standalone cyber insurance. This coupled with growing data around cyber risk, will also promote further development of differentiated cover, and encourage new insurers to enter the market.

While the Enterprise Internet of Things is set to deliver new value to businesses through unprecedented volumes of valuable data, it also gives rise to new vulnerabilities and risks.

Likewise, the rapid move by organisations to move to the cloud — many already ridding themselves of their own data centres — raises another interesting set of questions about third party service providers and their levels of security and limits of liability.

Contact

Fergus Brooks
National Practice Leader – Cyber Risk
+61 2 9253 7835
fergus.brooks@aon.com

Empower Results®