NOTEBOOK

No better time to buy cyber insurance

As ransomware and data breach incidents hit the headlines more frequently, the dangers of 'silent cyber' continue to lurk. Yet insurers are starting to get a handle on insuring cyber and are ever more enthusiastic about its potential, while the cyber insurance market continues to grow in tandem with an increasing awareness from clients.

By Chia Wan Fen

The cyber insurance market in Asia-Pacific could potentially grow to reach $1bn in premiums by 2025, according to keynote speaker Delta Insurance New Zealand managing director Ian Pollard. Currently, Delta, the first cyber and technology Lloyd's coverholder in Asia, estimates the APAC market to be worth over $100m, but could reach $250m by 2020 with more understanding and solutions addressing cyber risk.

"There is no better time for buying cyber insurance. Coverages are broad and premium rates are competitive," said Mr Pollard, who pointed out that less than 5% of businesses in Asia hold specific cyber insurance policies, compared to 14% in Australia and 10% in New Zealand respectively.

However, he noted that with more claims and cyber risk data and changing legislations, there would eventually be a rate hardening as the industry has a better understanding of cyber exposure.

Threats to watch

In terms of evolving threats, he highlighted data breaches as one to watch, in view of major incidents recently like the SingHealth breach in Singapore, and increased complexity of the issue due to GDPR compliance requirements. Delta estimates the minimum costs of a breach to be at least an insurable $5m, excluding spillover costs like technology improvements or business interruption.

Another prominent threat, ransomware has increased 167 times year-on-year for the last three years and now generates $1bn a year for criminals, while 'cryptojacking', which is the practice of hijacking computers to mine cryptocurrency, saw an 85-fold increase in 4Q17 coinciding with the spike in bitcoin prices.

Describing cyber resilience as comprising of public/private cooperation, risk management and cyber risk protection, he said the first in particular needs to increase, and it should be organised and led by governments—Singapore's, he highlighted, is doing a good job of this.

Claims and underwriting

Cyber continues to expand and it is increasingly being viewed as a peril, said AIG EMEA head of cyber Mark Camillo. It is moving towards affirmative coverage across multiple product lines, such as K&R when it comes to cyber extortion like ransomware. Meanwhile, cyber claims continue to increase significantly. The largest segment of buyers still comprise financial institutions, but interest from other sectors is growing.

Mr Camillo said that the industry is shifting focus from post-incident to pre-loss prevention services like employee cyber security education and vulnerability scans to help avoid a breach in the first place and create an end-to-end risk management solution. An increase in regulatory scrutiny, he said, has and will result in more transparency in the underwriting process with enhanced questionnaires. On the other hand, insurers now have to address questions like sophisticated clients asking how their enhanced security and controls could possibly influence their premium rates.

Regulation will also put more

pressure on the industry to exercise clarity in addressing non-affirmative silent cyber coverage, while industry members are starting to share information on how they perceive cyber risks with clients, which is very valuable for the latter to seek board approvals on the cyber security investments that are most suited to them.

'Silent' cyber

Indeed, the topic of 'silent cyber' was discussed by many speakers including Kovrr CEO Yakir Golan. Silent cyber is the potential loss due to cyber incidents that occur within insurance policies across multiple business lines not specifically designed to cover cyber risks.

"With the increasing exposure of traditional lines to cyber-related events—that's where the real hidden costs are," Mr Golan said. "With these events not priced into policies, what's not defined comes down to interpretation."

He said that the greatest challenge in silent cyber is quantifying it, and his view is that insurers should not to be too eager to launch new affirmative cyber products if they do not yet have a full understanding of the capital at risk in their books.

"There is a genuine need in the market for a fully integrated bespoke solution for managing silent cyber risk exposure…modelling this must be fully tailored to each one's processes, matched with relevant data against the cyber threat landscape," he said.

'Blended' policies

Some companies do actively choose 'blended policies', the most common blend being PI and cyber coverage with common aggregates that cover 'silent cyber' within. These blended policies are often chosen over standalone cyber policies due to price considerations. Otherwise, insureds sometimes choose to engage in 'cyber buybacks', for the policies they have chosen which feature cyber exclusions, said Munich Re Syndicate Asia Pacific head of financial lines & business development Joel Pridmore, who cautioned against doing so just to prioritise the price of the policy over the scope of coverage.

He explained that often professional services firms are required to hold certain PI limits to comply with contractual obligations to their clients. Should a major data breach occur, the blended PI/cyber tower could suffer complete erosion, thereby eliminating the PI cover of the firm and breaching their contracts with clients, thus resulting in costly class action proceedings.

He said that the option of cyber buybacks may also have gaps. For example, the wording may be limited and not cover incidents which are not targeted at the insured, but instead occur due to reasons like malware.

Risk management

Commenting on the modern risk landscape today, Mr Thomas Herde, Guy Carpenter's managing director, head Casualty Specialty Practice (Asia-Pac), said that companies are currently covered for only 15% of potential cyber-risk losses, against 59% for property, plant and machinery losses.

Given the worth of intangible assets today compared to traditional physical assets, companies ought to do more to protect themselves against 'intangible risks' such as reputational risk, he said.

From a risk management perspective, he also noted how insurance companies should be aware of the prospect of overlapping cyber liabilities from the traditional classes they underwrite.

In the absence of a special clause it is often extremely difficult to determine first, whether all losses have arisen from one event or cause, and secondly, precisely what that event or cause is. Therefore for cyber, he said the only sensible way of resolving the difficulty is by having recourse to an aggregate reinsurance structure which does away with the necessity of looking for a single common underlying event or cause.

"It is prudent to have an overarching cover in case specific event covers don't work," said Mr Herde.

SMEs

Asked about how the small and medium enterprises (SMEs) with limited resources should deal with cyber risks, Horangi deputy director of cyber operations Mark Fuentes said that there are low-cost measures for them to educate themselves, such as through online research.

PwC Singapore digital trust leader Tan Shong Ye suggested that SMEs could put their servers in the cloud, as "there's more expertise out there". He cautioned, though that while a company's main systems can be in the cloud, there is a lot of end users' data and use of their own devices via the Internet of Things and wireless connections which will not be covered. This, Mr Tan said, also points to how cyber threats are shifting.

Cyber as transformation

Despite the multiple cautionary notes, speakers urged the audience to view cyber risk and cyber security as enablers, not just through cynical lenses as disruptors or inhibitors. Right now, the world is standing at an inflection point where companies must adopt new technologies to succeed as a 21st century enterprise, or perish. But in their digital transformation, cyber security transformation must keep pace, or that gap becomes cyber risk, said KPMG Advisory LLP Partner and head of cyber security Daryl Pereira, as adopting emerging technologies creates risks.

"As you fund and invest in innovation, you must fund and invest in cyber security transformation in lockstep," he said. APAC CEOs are still playing catch-up to global counterparts in terms of emerging tech adoption and preparedness for a cyber security event. In their business strategies to transform, they must have cyber security built within all projects, he said.

DXC Technology general manager for security Abdallah Zabian said that cyber insurance is transforming into an essential offering and potential revenue stream for insurers due to complex cyber threats and government regulation.

"We need to leverage our cyber partners not only to mitigate risk but also to look at them as a potential to increase your revenue. I know that cyber is going to enable insurance, but the insurance industry will revolutionise and transform the maturity of cyber across the world," he said.

The 3rd Asia Cyber Risk Summit, sponsored by Singapore Re, was held in Singapore from 17-18 September and drew some 120 participants.