CYBER INSURANCE MARKET INSIGHTS

Q4 2019

AON

Empower Results®

OVERVIEW

Cyber risk and cyber insurance continue to gain attention. Cyber attacks and data breaches was revealed as the number 5 risk for Australian businesses in Aon's 2019 Global Risk Management Survey. Recently we have witnessed significant cyber claims manifesting, in some instances rapidly, both in Australia and around the globe.

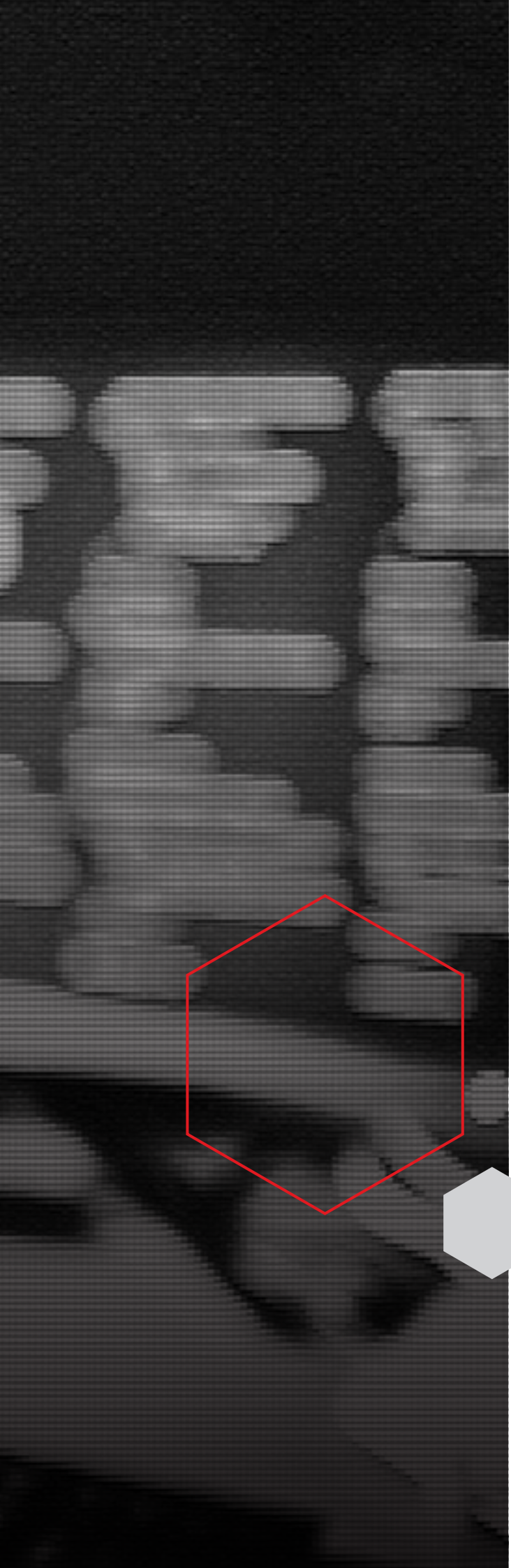
The Australian cyber insurance market continues to grow. Aon estimates the local cyber insurance market now exceeds $100 million. Grand View Research estimates the global cyber insurance market is valued at US$4.3 billion[1].

- General Data Protection Regulation (GDPR) has wide ranging implications. Recently, we have seen a willingness of the regulator to impose significant fines against European and US headquartered organisations. For example, British Airways and Marriott were both fined £183 million[2] and almost £100 million[3] for recent data customer breaches. Australian companies could also be at risk.

- The local privacy regulator, Office of the Australian Information Commissioner (OAIC), has taken a more consultative and informative approach by releasing quarterly and yearly reports on the types of breaches and attacks being reported in Australia. The first annual report from Australia's Notifiable Data Breaches scheme revealed that there were 964 eligible data breaches reported in the first 12 months of the scheme[4]. However, there are proposed amendments to the Privacy Act which will increase the power and authority of the OAIC more closely aligning to the EU's GDPR. The proposed amendments will increase the maximum financial penalty for breaches to $10 million (up from $2.1 million). The OAIC will also be granted another $25 million in additional funding to investigate and respond to breaches[5].

- Data breaches have resulted in some of large losses to the industry over the last 12 months. However, business interruption losses and the speed at which they manifest is causing the greatest concerns to insurers in 2019. There is no requirement to notify business interruption incidents to the OAIC that haven't involved a data breach, so it is highly likely that losses to the insurance industry will not align to the facts reported by the OAIC.

[1] https://www.grandviewresearch.com/industry-analysis/cyber-insurance-market
[2] https://www.bbc.com/news/business-48905907
[3] https://www.theguardian.com/business/2019/jul/09/marriott-fined-over-gdpr-breach-ico
[4] https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/
[5] https://www.rigbycooke.com.au/tougher-penalties-to-be-introduced-under-the-privacy-act/



STATE OF THE MARKET

2019 saw global and local growth in the cyber insurance market. However, some losses saw insurers start to focus on appropriate premiums and retentions for individual risks. Norsk Hydro - one of the world's largest aluminium producers - suffered an attack earlier this year which caused production outages across Europe and the US[6]. Combine that with a number of other high profile IT failures in the digital infrastructure arena - such as Lloyds Bank[7] - has resulted in insurers now starting to consider appropriate rates and retentions to maintain profitability.

Compounding the impact of this is the NotPetya attack of 2017. This incident caused complications within the non-cyber insurance market, commonly referred to 'silent cyber', resulting in some of the most hotly contested insurer responses to cyber claims.

Australia is starting to witness large losses being paid under cyber policies. Insurers are now facing multiple losses across multiple industries, ranging from education (Australia National University[8]) to professional services (Landmark White[9]) through to manufacturing and healthcare. Some of these losses exposed little personally identifiable information and therefore have not been reported in the media. However, the business interruption losses have been significant. This is a driving force for insurers to realign their focus on profitability.

Insurer globalisation has reached new levels with continued market merger and acquisition activity. Combine that with losses - both frequency and severity - and we are starting to see that impact the available capacity. As a consequence, and considering the broader insurance market fluctuations, cyber insurance may be starting a transitionary cycle.

[6] https://www.bloomberg.com/news/articles/2019-03-19/hydro-says-victim-of-extensive-cyber-attack-impacting-operations-jtfgz6td

[7] https://www.theguardian.com/business/2019/feb/11/lloyds-apologises-after-customers-hit-by-online-banking-glitch

[8] https://www.anu.edu.au/news/all-news/anu-releases-detailed-account-of-data-breach

[9] https://www.lmw.com.au/about-lmw/news-updates/data-disclosure-incident/

CYBER INSURANCE MARKET SNAPSHOT

CLAIMS & LOSSES	COVERAGE	CAPACITY	RETENTIONS	PRICING
↑	↑	↔	↔	↔
Significant losses have been identified in the market, whilst frequency continues to grow	Coverage continues to evolve and become more valuable	Capacity shows signs of contraction following global mergers / acquisitions and claims	Retentions are being reviewed	Pricing trends are stabilising, scrutiny increasing over existing programmes

Ransomware

Ransomware has gained interest from insurers and the media given the frequency and severity of claims and incidents. Beazley recently reported that the number of ransomware incidents has increased by 37 percent[10]. It is worth comparing the incident response component of a cyber policy to a kidnap and ransom policy. Cyber insurance provides insureds access to an 'A Team' if an incident was to arise, including access to incident response and investigation teams as well as reimbursement of crisis communications and reputational mitigation costs.

These types of incidents, along with cybercrime in general, are causing the market concern. Cybercrime is now reported to be the fastest growing form of crime in the US, and by 2021 is predicted to be more profitable than the global trade of all major illegal drugs combined.[11]

LOOKING AHEAD

Silent cyber is likely to dominate the landscape for the following few years. Insurers will continue to grapple with the intent of existing policies. They will have to decide if their traditional policies will affirmatively respond or exclude cyber incidents.

Allianz is a global leader in addressing this exposure. They are in the process of identifying the exposures and addressing traditional policies to unambiguously address whether cyber exposures will be covered under their property and casualty policies[12].

We expect each insurer to undertake a similar process. This could be a challenging process for clients in the short-term, however it is critical that all insurers undertake this review to understand their accumulated exposures.

Couple this with a growing sample set of large cyber losses across multiple industries and the continued and unrelenting prevalence of ransomware and phishing attacks, the cyber insurance market is set to continue to grow at a significant rate.

Historically, early adopters of cyber insurance have benefitted from lower than average premiums and retentions. Insureds can expect some pressure on retentions and/or premiums in the coming 12 months. Most insurers are looking to 'right size' retentions, and from our experience, several of our early adopter clients are experiencing small rate increases.

Coverage has been expanding continuously since its inception and this trend is likely to continue. Other lines of insurance, such as property, general liability and kidnap and ransom, are showing some signs of potentially restricting coverage for cyber perils, and the ubiquitous use of technology. In certain circumstances, cyber insurance may fill gaps left by other lines of insurance.

Intangible assets are a critical component of an organisation's balance sheet. In fact, intangible assets now represent nearly 85 percent of the value of the S&P 500. The 2019 Intangible Assets Financial Statement Impact Comparison Report shows that only 16% of informational assets are covered by insurance, compared with 60% of potential property, plant and equipment assets. Cyber insurance is a key ingredient in protecting informational assets.

As other markets continue to show signs of instability, cyber insurance will continue to evolve to the new risk landscape and be seen by insureds as no longer a discretionary insurance policy but rather one of their most critical insurance policies.

[10] https://www.beazley.com/news/2019/beazley_reports_a_37_rise_in_ransomware_incidents.html
[11] https://www.prnewswire.com/news-releases/cyberattacks-are-the-fastest-growing-crime-and-predicted-to-cost-the-world-6-trillion-annually-by-2021-300765090.html
[12] https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/silent-cyber.html

Contact

Michael Parrant

Cyber Insurance Practice Leader
+61 3 9211 3485
michael.j.parrant@aon.com

© 2019 Aon Risk Services Australia Limited ABN 17 000 434 720 | AFSL 241141 (Aon)

This information is intended to provide general insurance related information only. It is not intended to be comprehensive, nor does it, or should it (under any circumstances) be construed as constituting legal advice. You should seek independentlegal or other professional advice before acting or relying on any of the content of this information. Before deciding whether a particular product is right for you, please consider the relevant Product Disclosure Statement or contact us to speak to an adviser. Aon will not be responsible for any loss, damage, cost or expense you or anyone else incurs in reliance on or user of any information contained in this document.

Empower Results®