Cyber Insurance Market Insights – Q3 2018

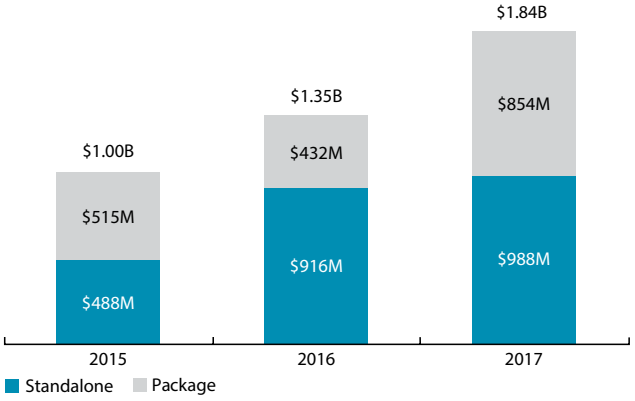
Overview

- The cyber insurance market is maturing and penetration rates are improving in Australia
- Local cyber insurance market size is estimated to be approximately $60 million, with the global market estimates ranging between USD3 billion - $3.5 billion
- Since the implementation of Notifiable Data Breaches (NDB) scheme on 22 February 2018, the Office of the Australian Information Commissioner (OAIC) has already been notified of 305 data breaches[1] up to 30 June 2018
- In 2018, Australia commenced what will go down in legal history as the Year of Global Privacy Legislation[2] by implementing our new regulatory regime, following the global trend of expanding regulatory oversight concerning privacy. Additional legislation being enacted globally includes:
  - Europe's General Data Protection Regulation (GDPR) was implemented regulation in May
  - Last two USA states (South Dakota and Alabama) implemented regulation in Q1
  - California implemented the California Consumer Privacy Act 2018 in June which imposes restrictions on companies trading in information
  - In November, Canada will implement the long awaited Personal Information Protection and Electronic Documentations Act.

State of the market

2017 saw significant local growth in the uptake of cyber insurance, Aon estimates the market grew nearly 100 per cent compared to 2016. Whilst the market is still relatively small, similar growth is expected in Australia for the coming 2-3 years. The current and expected growth trajectory exceeds those expectations for almost all developed countries, including the US where the market grew by 37 per cent on the prior year.

Exhibit 1: US cyber direct written premiums 2015 - 2017



Source: Aon Benfield

[1] https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports/notifiable-data-breaches-quarterly-statistics-report-1-april-30-june-2018
[2] https://www.jdsupra.com/legalnews/canada-s-new-data-breach-notification-41990/

Over the past five years, cyber premiums have grown significantly. Exhibit 2 predicts that by 2022, worldwide cyber premiums will be worth $7 billion, a compound annual growth rate of 15 per cent.

These projections may be exceeded following the outcomes of the 'silent cyber' reviews being enforced by Lloyds of London on its 80+ Lloyds syndicates, and the worlds' rating agencies requesting similar reviews on global insurance companies. This review is designed to ensure all markets understand the cyber exposures covered under existing lines of insurance, and either affirmatively cover and charge for the exposure, or exclude coverage.

Bespoke cyber solutions are being crafted to meet the specific demands of clients as well as in anticipation of the above reviews. Cyber insurance is now proactively filling gaps in insurance programs, including some 'silent cyber' exposures that clients are now looking to proactively address. A carefully constructed cyber policy may now be implemented which caters to:

- Property Damage / Bodily Injury
- Environmental Liability
- Cyber Terrorism
- Reputational Harm
- Fines & Penalties, beyond Privacy Regulator breaches
- Failure to Supply coverage

Some of the reasons organisations no longer want to rely on 'silent cyber' coverage include:

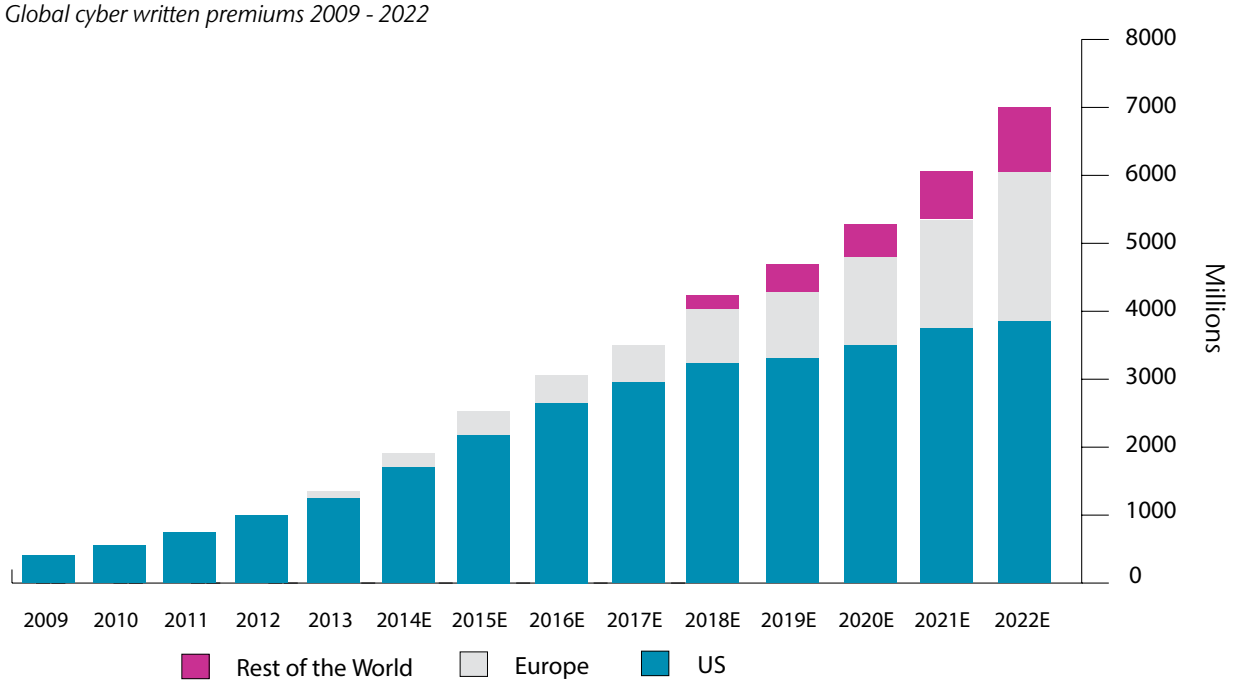
- The 2017 WannaCry and NotPetya ransomware attacks have crippled some organisations, and some have found their current insurance programs lacked the response they required
- Boards are looking for affirmative coverage, especially given the challenges faced by Merck and Maersk to name a few
- With the development of technology and specific exposures, organisations are looking to protect their traditional lines of insurance from the impacts of a cyber event, and specifically ring-fence as much exposure into the emerging class as possible.

Local rates continue to be competitive, however there is a measure of caution in the Australian market for the potential impacts of aggregation styled exposures. This caution is compounded when combined with broader coverage such as system failure. Caution is warranted given the frequency and severity of claims we are witnessing globally. With the local market estimated to be approximately $60 million, there needs be only a few sizeable claims to impact the entire local market.

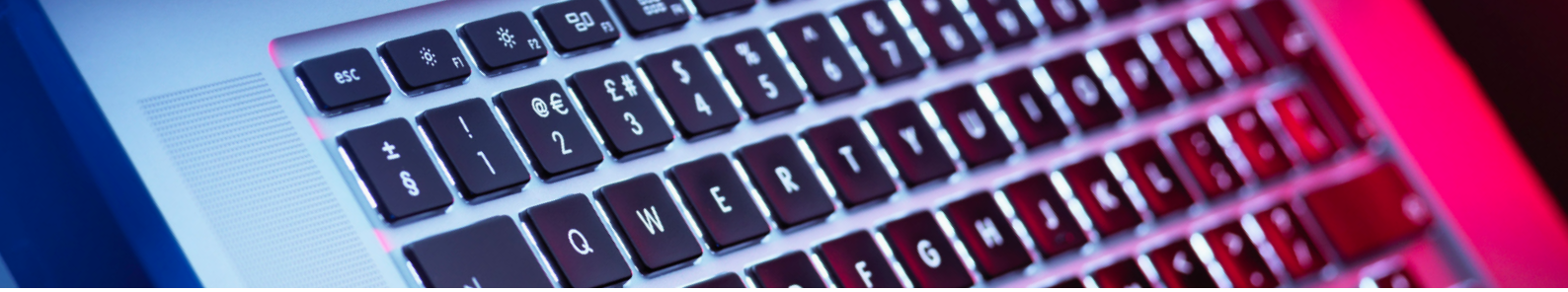
What is silent cyber?

Silent cyber refers to a situation where cyber risk exposure is assumed by default (but not expressly included) within policies such as property, marine or liability. The most common case of 'silent cyber' is where the policy does not clearly exclude cyber coverage.

Exhibit 2: Global cyber written premiums 2009 - 2022



Source: Betterley, Aon, Westhouse estimates



New data breach legislation – global changes and impacts

Australia now lives under a new data privacy regime since the introduction of the NDB scheme on 22 February 2018. Under the regime, it has become mandatory for various organisations and government agencies to notify individuals, and the OAIC, of data breaches that are likely to result in serious harm.

To the 30 June, the OAIC has been notified of 305 data breaches. During the period of 1 April - 30 June 2018, the OAIC received 242 data breaches. Of those 242 reported breaches, the majority involved 'contact information', such as individual's home address, phone number or email address. Also, 59 per cent of data breaches during this quarter were attributed to malicious or criminal attacks. Human error remains a major source of breaches, accounting for 36 per cent of those 242 data breaches.

Financial penalties for failure to report an eligible breach include fines up to $420,000 for individuals and $2.1 million for organisations. Whilst such fines may seem pecuniary against companies, the reputational harm and business interruption impacts may be ruinous.

Whilst adapting to the new NDB laws may be challenging, keep in mind the daunting prospects of complying with the GDPR. The GDPR enforces 72 hour notification provisions, and the extremely steep penal fines of up to EUR20 million or 4 per cent of global revenues (whichever is higher). Further, if you are operating in any way within the US, note that every state now has their own respective data breach legislation. Each state operates independently of each other with no Federal equivalent.

Preparing for an incident

Despite clear direction from the OAIC as to how to manage an incident, many Australian businesses remain underprepared. According to CSO 1 in 5 affected Australian small and midsize businesses are forced to close their doors following an attack[3].

A robust approach to risk management revolves around building solid defences to cyber-attacks, however many progressive organisations budget an equal portion to defence as they do to incident recovery.

A portion of the budget for recovery will often be set aside for testing the incident response plan. Best-in-class plans will include third party experts to enhance the testing environment and improve the final output. Whilst nothing can definitively prevent a cyber incident from occurring, proactively planning and testing for a real world worst-case scenario will help limit the damage to brand and reputation and business interruption.

Looking ahead

As more people and devices connect across the globe, the risk and impact of data breaches from malicious cyber-attacks, system failures and human error will only continue to increase.

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.

Contact Us

Michael Parrant
Cyber Insurance Practice Leader

+61 3 9211 3485
michael.j.parrant@aon.com

[3] https://www.cso.com.au/article/625556/ransomware-forces-1-5-affected-australian-smbs-close-their-doors/