CYBER INSURANCE MARKET INSIGHTS

Q3 2020

AON

OVERVIEW

Cyber risk and insurance continue to dominate boardroom discussions with cyber criminals taking advantage of the confusion emanating from the COVID-19 pandemic, and technology being increasingly acknowledged as a critical component of business success.

In March 2019 the Australian Government announced its intention to increase the maximum penalty applicable to a corporation's serious breach of the Privacy Act[1]. The increased penalty will align with the maximum penalty currently available under the Australian Consumer Law - the greater of either $10m; three times the value of any benefit gained as a result of the contravention; or 10% of annual turnover.

The intention to increase penalties is a herald that government and regulator attitudes are changing; where previously the focus was on awareness and education, that focus is now shifting towards enforcement. These reforms have not been enacted yet, but rather are on the cards for the future.[2]

Further, the implementation of consumer data rights as of 1 July 2020 for certain industries[3] and the 14 May 2020 amendment to the Privacy Act to expressly protect COVIDSafe app users[4] demonstrates the Australian Government's hardening position on data protection.

The cyber insurance market continues to evolve, with ransomware events causing major concern for cyber insurers. The list of global cyber incidents, many of which have insurance, is staggering:

- Data breaches stemming from university use of exam Proctor software
- The Australian Prime Minister's announcement of ongoing state-sponsored attacks
- Cyber incident involving the Victorian healthcare sector
- Norsk Hydro's ransomware incident was a watershed moment for non-traditional cyber insurance purchasers
- Multiple incidents in the airline industry, including British Airways, Cathay Pacific and EasyJet
- Incidents across manufacturing, logistics and associated industries, including Toll, Mitsubishi and Honda
- ASIC taking action against a financial institution for inadequate cyber security systems

Unfortunately, this list is a very small subset of the global cyber incidents that have been witnessed over the last 12 months. Some markets are reporting 'no less' than 20% uplift in ransomware events alone in the last three months, with others witnessing and reporting on this trend as early as Q1 2020[5]. However, the extremely challenging change has been the financial consequences of ransomware events which have reportedly increased 10 times compared to 12 months ago.

These events are the types of events that cyber insurance will typically respond to, and for which insurers are watching carefully. As the frequency and severity of these events escalate at an alarming pace, impacting all types of organisations, irrespective of their individual or industry maturity, insurers will start to move from education to enforcement when it comes to preventative measures and an improving risk posture.

1 https://www.attorneygeneral.gov.au/media/media-releases/tougher-penalties-keep-australians-safe-online-24-march-2019

2 https://www.lexology.com/library/detail.aspx?g=3909e617-a4f8-4ade-bea1-e8e328d76efc.

3 https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0

4 https://www.oaic.gov.au/privacy/covid-19/the-covidsafe-app-and-my-privacy-rights/

5 https://www.reinsurancene.ws/ransomware-attacks-up-25-in-q1-says-beazley/

CYBER MARKET OVERVIEW

Claims & Losses	Coverage	Capacity	Retentions	Pricing
Significant losses identified with frequency continuing to grow	**Coverage continues to evolve**	**Capacity continues to grow globally**	**Retentions being reviewed**	**Pricing trends stabilising, scrutiny increasing over existing programs**
Frequency and severity of ransomware continues to drive losses with frequency up significantly in 2020, however more alarmingly the severity of the damage is increasing by orders of magnitude Complexity of breaches and lack of competition has driven increase in incident response expenses eclipsing US costs Severity of BI incidents resulted in significant losses Increasingly punitive legal and regulatory environment emerging Cyber risk management seen as a major D&O consideration	Wannacry, NotPetya and Ransomware incidents re-focus attention on BI & supply chain exposure Insurers continue to update policies to meet evolving coverage needs Emphasis on pre-arranged vendors Some contraction around certain covers if claims continue on the same trajectory War & terrorism still a point of contention Silent cyber is a huge topic – the market will be pressed to assist with an insurance solution	Over 75 unique insurers providing cyber capacity Capacity available locally, in London, Bermuda and Asia. Insurers reviewing aggregate/accumulation exposures Over $1bn theoretical capacity available, however insurers starting to focus on limit management Contractions on line sizes being considered by some markets Carriers more discerning about where and how much capital they deploy Average limits purchased is up 42% for large companies over a 36 month period	Significant retention adjustment may lead to increased cover and/or pricing flexibility Earlier adopters seeing pressure applied to 'right-size' retentions compared to similar new adopters Critical infrastructure organisations consider large retentions in exchange for tailored (broad) coverage Some carriers revising minimum retentions for certain industry verticals As ransomware frequency increases, more carriers wish to lift themselves out of 'attritional' loss zone	Premiums trending 5-15% increases due to deteriorating claims and markets considering long-term stability Excess market show trends of rate increases of 10% or higher, especially for large companies Strong local and global market appetite still exists, however ratings considered Some organisations have secured significant cover improvements as a result of higher premiums

STATE OF THE MARKET

Whilst capacity is still readily available to Australian organisations, markets are now looking at sustainability as a priority. The rapid impact of cyber incidents is giving pause to insurers, prompting reconsideration of how cyber insurance should be modelled, potentially moving away from the traditional long tail insurance model and aligning more to short tail insurance models due to the rapid manifestation of losses.

This is an important concept to the insurance industry as it dictates how profitability and reserving are defined for insurers. To provide a sustainable insurance solution, insurers need to realign their understanding of how rapidly their capacity may be consumed. When combined with the now frequent and devastating impacts of ransomware, insurers are considering how their premium pricing models need to be developed.

Despite the challenges faced by organisations due to economic uncertainty and the ongoing impacts of the COVID-19 pandemic, cyber risk and insurance is still receiving significant attention. In part this is likely due to the further heightened importance of technology as a revenue stream.

2020 will see an increase in cyber insurance higher than historical increases. Aon has seen premium and policy count increase year-on-year from 2012 of circa 30%, however 2020 is already trending at 50% growth compared to 2019 despite the economic uncertainty. This is due to a combination of three factors:

- Premium rate increases – organisations can expect to see a 10% uplift in premium for their same program limits. This is in part due to the transitioning market, as well as historically competitive premiums
- Increased limits – many organisations that have purchased cyber insurance for a number of years and are familiar with the coverage, are looking to increase their limits to more accurately reflect their risk
- Heightened awareness – will result in a large increase in new purchasers throughout the year, across all industry sectors, and organisation sizes

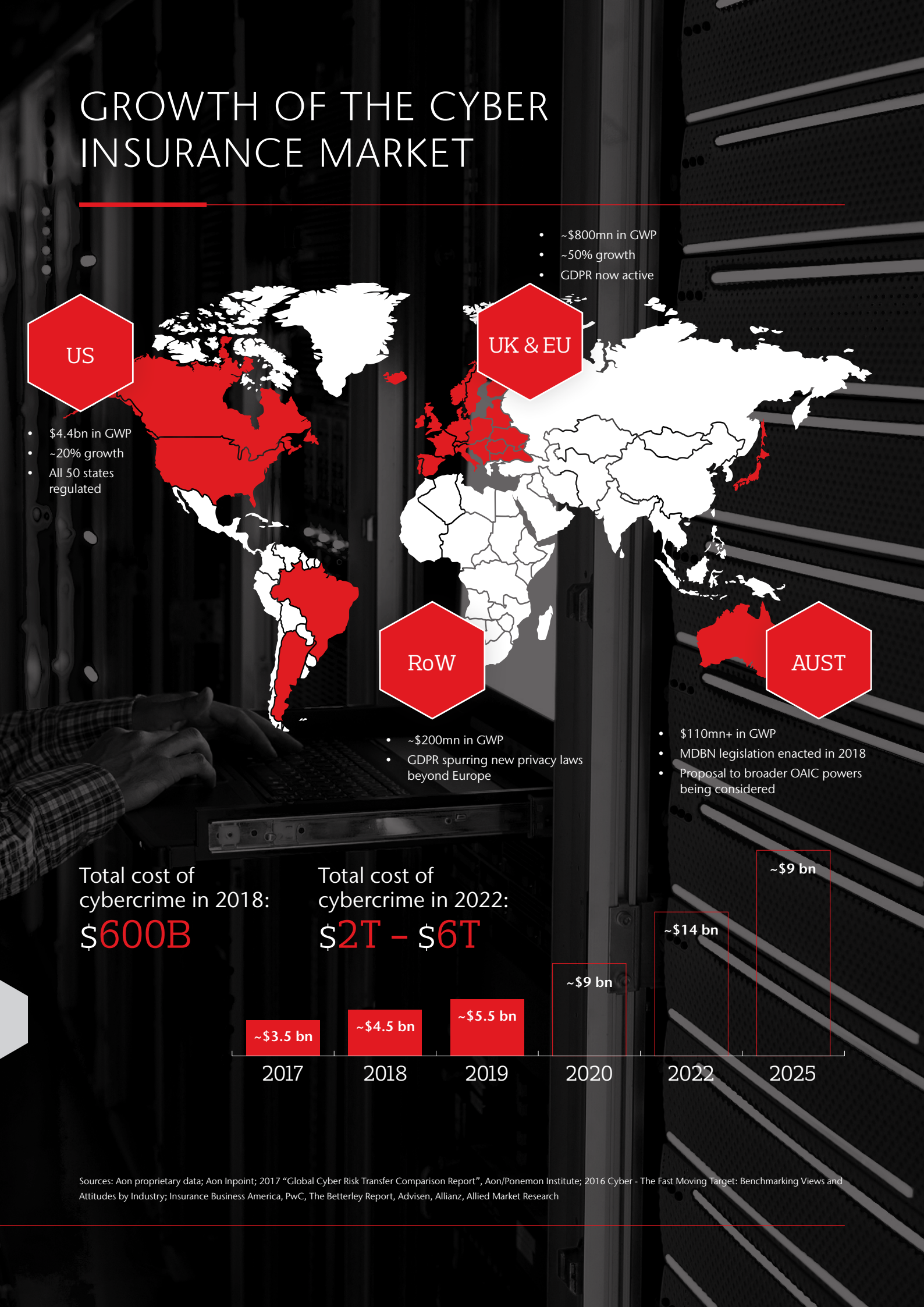
Cyber insurance

projected to grow from

$5.5 bn at year-end 2018

to $20 bn by 2025.

GROWTH OF THE CYBER INSURANCE MARKET



Total cost of cybercrime in 2018:
$600B

Total cost of cybercrime in 2022:
$2T – $6T

Sources: Aon proprietary data; Aon Inpoint; 2017 "Global Cyber Risk Transfer Comparison Report", Aon/Ponemon Institute; 2016 Cyber - The Fast Moving Target: Benchmarking Views and Attitudes by Industry; Insurance Business America, PwC, The Betterley Report, Advisen, Allianz, Allied Market Research

LOOKING AHEAD

Silent cyber[1] has truly become a topic of discussion for all lines of insurance. Whilst the consequences of silent cyber are more keenly felt in other lines of insurance, cyber insurance will be challenged to provide solutions. As a major issue for the entire market, we anticipate alternative cyber solutions will emerge as mainstream options in the future, providing solutions where other lines of insurance have retracted from the emerging exposure.

Alternative risk transfer markets and options will become more common as limits of indemnity exceeding $1bn become more essential, whether for traditional cyber or alternative cyber solutions providing broader coverage such as actual bodily injury, property damage or environmental liability to name a few.

Silent cyber will continue to be a challenge to be managed by the industry. As a result, organisations will need to start reviewing their limit requirements and look to structure programs that maximise the available capacity to them for their critical exposures.

Ransomware will dominate the discussion. It cannot be overstated the impacts such attacks/losses are having on the cyber market. Insurers are still providing broad solutions to these incidents, however it is likely that insurers will need to reconsider their approach to this aspect of coverage. Insurers are likely to move from an educational approach to offering a wide range of non-insurance products and solutions designed to reduce the insured's and insurer's exposure to such attacks.

Insurers are likely to, over a handful of years, move to an enforcement regime where organisations must utilise certain products and services in order to gain insurance for ransomware events. These 'conditions precedent' have been mostly removed from cyber insurance, however unless wider action is taken to mitigate this type of attack, insurers will be forced to drive attitude change via a focus on providing superior terms and conditions to compliant organisations, and reducing their exposure to non-compliant organisations.

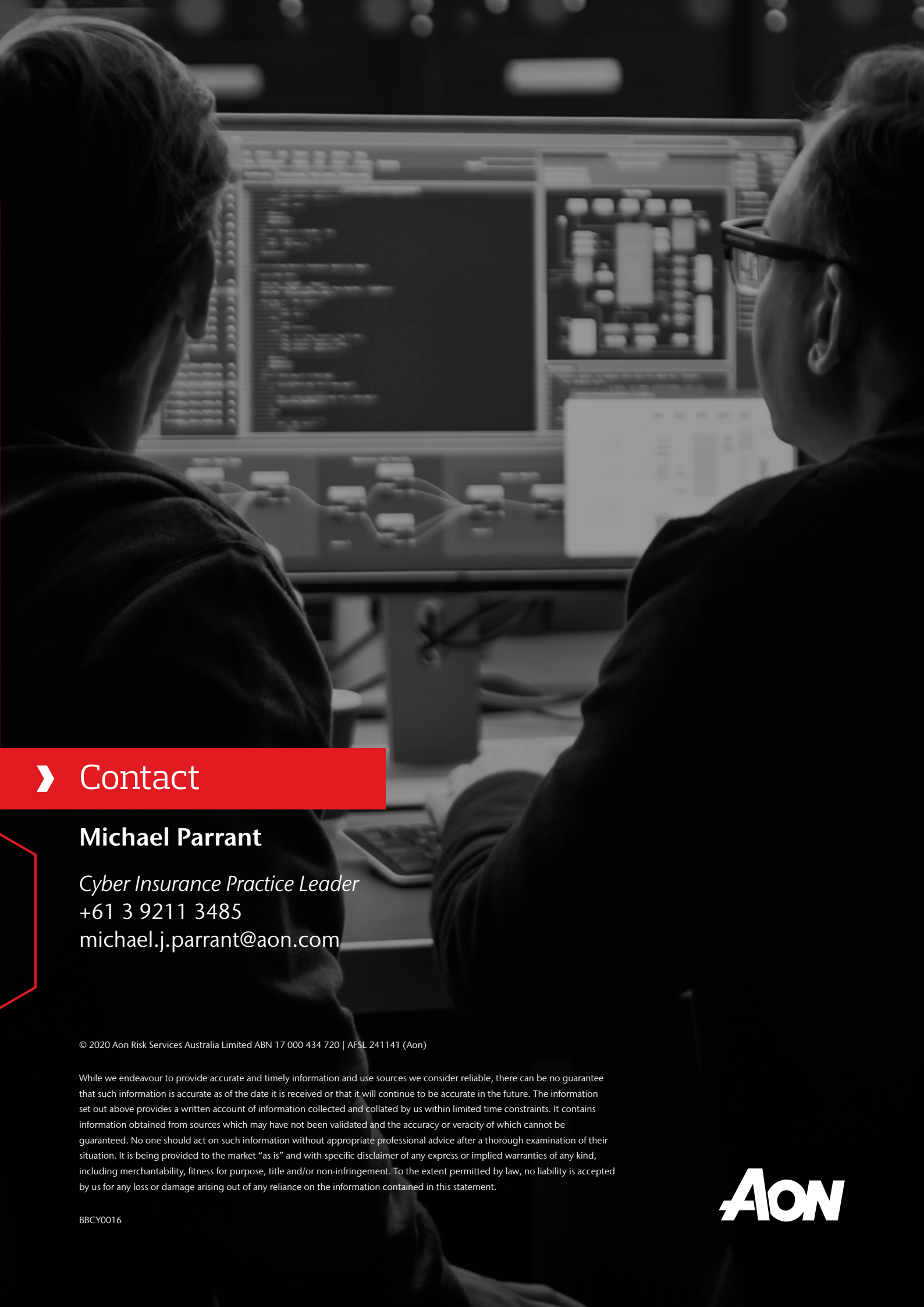
Ransomware

Ransomware has gained interest from insurers and the media given the frequency and severity of claims and incidents. It is worth comparing the incident response component of a cyber policy to a kidnap and ransom policy. Cyber insurance typically provides insureds access to a panel of incident responders 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[2].

1 Silent cyber refers to the cyber exposure existing in policies which do not specify whether losses arising from a cyber-attack are affirmatively covered.

2 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



Contact

Michael Parrant

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

BBCY0016