Marsh

Cyber Insurance

2021 Australian Insurance Market Recap Series

March 2022

At a glance

13%

Global commercial insurance prices rose 13% in Q4-2021 of 2021.

15%

Australia experienced a 15% increase in ransomware attacks from October 2020 to October 2021.
*(*Source: Australian Cyber Security Centre)*

Top 3 cyber claims

The leading causes of loss were:

- email or account manipulation fraud (61%)
- data breach (external),
- ransomware attack.

Ransomware attacks

Top 3 affected industries in 2021: legal, financial, and professional services.

22 days

The average downtime US organisations experienced following ransomware attacks in Q3 2021.

Rates

Cyber insurance prices increased at 101% in Q4-2021, with 98% of clients experiencing a price increase.

Government action

A new Ransomware Action Plan announced to protect individuals and companies from cybercrime.

Reforms to watch

Proposed new laws may force companies with greater than $10 million revenue to report any ransomware attack to the Government.

D&O risk

Cyber risk now has the potential to personally affect company directors and officers.

Coverage

More cyber capacity was placed through London based markets as fewer Australian insurers were able to write cyber insurance on a primary basis.

$ still worth it

Despite being a very challenging market, cyber insurance remains a very effective and cost advantageous transfer of this key risk.

Business proactivity a must

In 2022 insurers will require companies to demonstrate minimum security controls before insurance quotes are provided.

Cyber threat landscape in review

2021 was a tumultuous period in the cyber risk landscape, with the impacts of expanded threats, security challenges, and widespread changes to the way businesses operate.

The digital revolution transformed the way technology was utilised in daily life. To meet customer demands and drive efficiency, businesses have heavily invested in technology over the past decades to bolster production capacity and operational capability. This technology was tested during 2020 and 2021 when the global pandemic required businesses to re-evaluate the way they worked, from moving large portions of employees to remote work settings, to adapting different processes to adhere to new restrictions and government guidelines across the world.

Throughout last year, a number of zero-day vulnerabilities in software and applications were discovered, and in some cases exploited, by threat actors seeking to cause disruption for political or financial gain. Ransomware continued to be a significant concern for companies, flowing on to impact the cyber insurance market in a significant way. The average downtime experienced by US organisations following a ransomware attack, represented as a material interruption to operations or measured as less than 100% productivity, increased from 19 days in the third quarter of 2020 to 22 days in the third quarter of 2021[1]. Based on data from the Australian Cyber Security Centre (ACSC), Australia experienced a 15% increase in the number of ransomware attacks from October 2020 to October 2021.

Cyber risk and legislative changes

The publication of the 2020 Australian Cyber Security Strategy signaled an increasing focus by the Australian Government on cyber risk, with $1.67 billion to be invested over 10 years to improve online security for Australians. This included a commitment to work with industry to consider and clarify cyber security obligations.

To further their stance on cybercrime, in 2021 the Government announced it would take decisive action in protecting Australian individuals and companies from ransomware attacks, releasing a Ransomware Action Plan[2] outlining a series of objectives to address cyber risk and crime across three distinct categories: Prepare and Prevent, Respond and Recover, and Disrupt and Deter. Perhaps the most notable of the signaled legislative reforms is the mandatory ransomware incident reporting scheme. If introduced, it will require companies with greater than $10 million revenue to report any ransomware attack to the Australian Government.

Cyber risk and boards

Cyber risk is being discussed with increasing regularity and detail across Australian boardrooms. In addition to affecting a business' reputation, operations and/or financial performance, this risk now has the potential to personally impact directors and officers. Whilst not prevalent locally, cyber event driven class actions have been seen in overseas jurisdictions. Though based on a small sample size of US specific actions, the 2021 Full-Year Review of Securities Class actions by NERA Economic Consulting[3] showed cyber breach event driven class actions increasing from three in 2019 and 2020, to five in 2021.

As the threats emanating from cyber security risk grow, a significant challenge is facing company boards who are under pressure to be held accountable for failures to protect information assets and business operations from cyber security failures. Cyber risk moves quickly, and it evolves at a fast pace. There will be increasing expectations of company leaders to maintain a high level of responsibility for cyber risk issues and to have full oversight over its management. This may include improving cyber risk literacy and education at a Board level, or at a minimum having experts in place to guide decisions being made around investments into security and technology transformation projects.

1 Coveware. (October 21, 2021). Average duration of downtime after a ransomware attack from 1st quarter 2020 to 3rd quarter 2021 [Graph]. In Statista. (Retrieved Feb14, 2022, from https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/)

2 https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf

3 NERA Economic Consulting 'Recent Trends in Securities Class Action Litigation: 2021 Full-Year Review'

Cyber risk transfer

Cyber claims

A snapshot of Marsh cyber claims for the first half of 2021 showed that there was nearly a 50% increase in the number of cyber claims compared to the same time period in the previous year. The top three leading causes of loss were data breach (caused by an external threat actor), ransomware attack, and email or account manipulation fraud, which made up 61% of the cyber claims notified to insurers in 2021.

Consistent with insurer data, claims frequency increased slightly but more telling was the significant increase in the severity of a cyber claim.

In particular, for claims notified to insurers in 2021, where the leading cause of loss was a ransomware attack, it was found that:

79%
of cyber claims included a data exfiltration component

$60,000
Lowest ransom demand

$7,200,000
Highest ransom demand

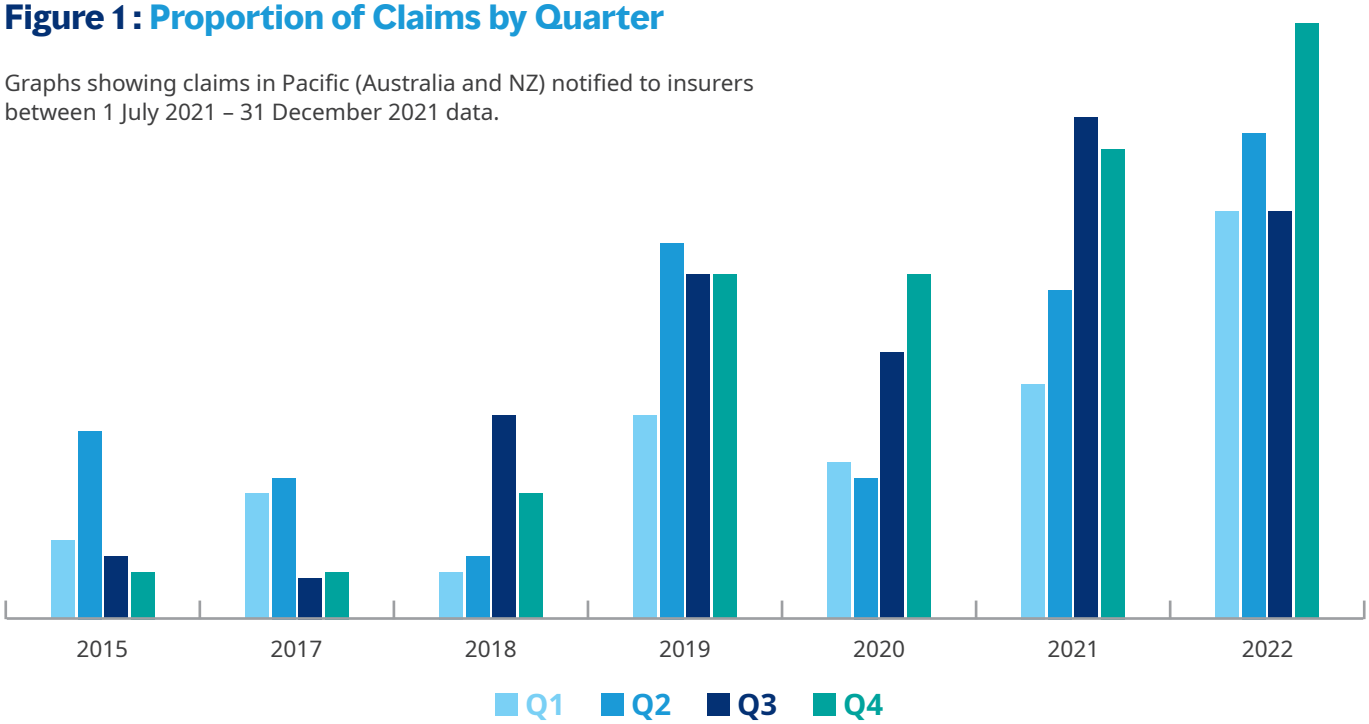
$2,686,344
Average ransom demand

TOP 3
affected industries were legal, financial and professional services

42%
of claims involved the insured pursuing business interruption loss as a result of the ransomware attack

Figure 1 : Proportion of Claims by Quarter

Graphs showing claims in Pacific (Australia and NZ) notified to insurers between 1 July 2021 – 31 December 2021 data.



Cyber insurance

Cyber insurance remains a very effective and cost advantageous transfer of this key risk. As noted above, cyber claims are occurring regularly and cyber wordings remain responsive to key triggers. For this reason, through 2021 insurers applied corrections to their cyber portfolios swiftly to stay ahead of deteriorating loss ratios in a unique class of business that includes both short-term and long-term claims tails.

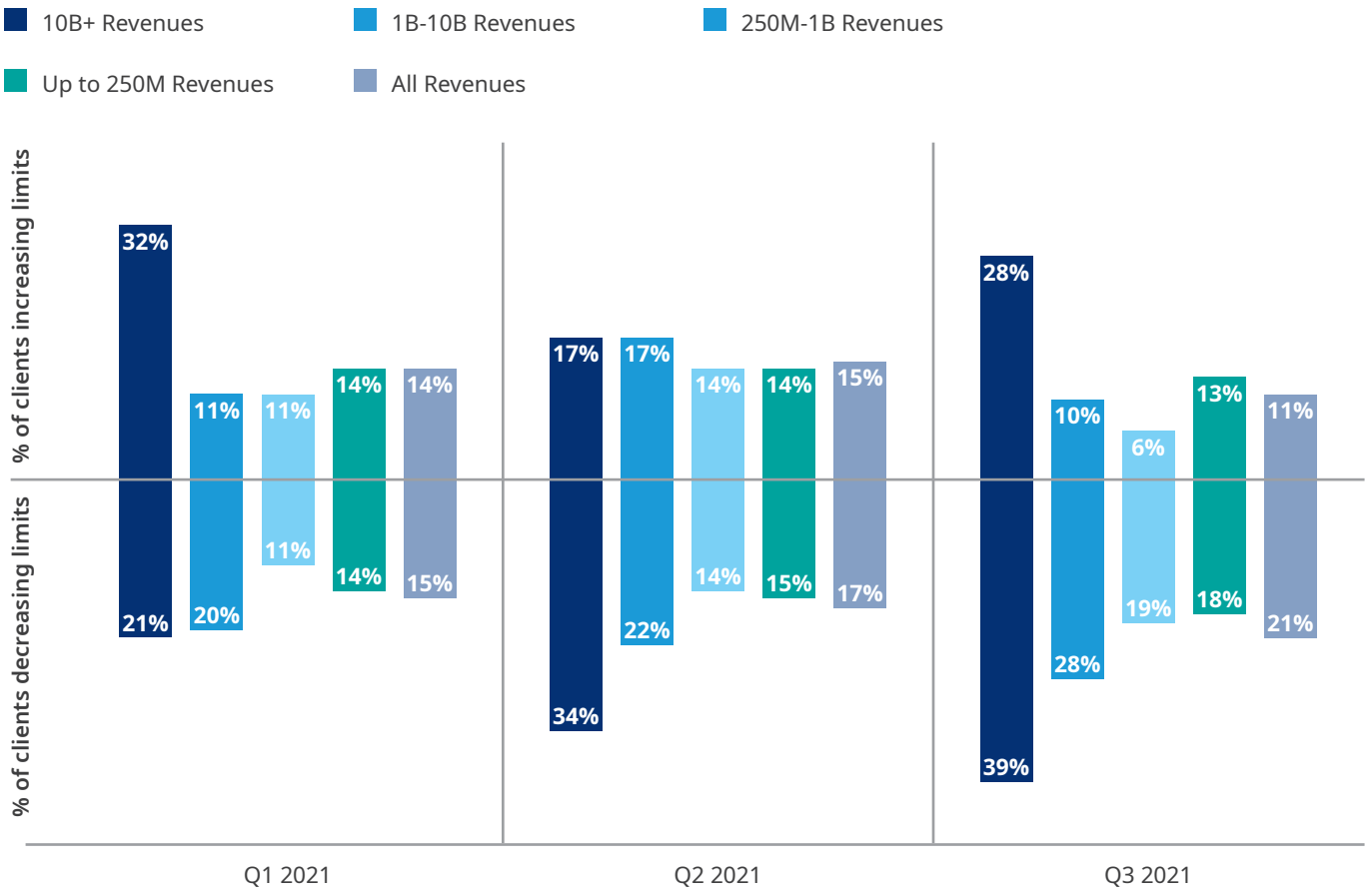
The National Association of Insurance Commissioners (NAIC) reported that in 2020, the average direct loss ratio for cyber coverage across the Top 20 US carriers was 66.9%, up from 44.6% in 2019. From regular market engagement across last year, Marsh postulates that insurer combined loss ratios for cyber exceed, or are very close to, 100% for a number of markets.

There remains an excess demand for cyber insurance compared to available supply in the market. Looking specifically at the limit purchasing profile of clients, Marsh US data shows progressive limit decrease through 2021, but also that limit increases were still being pursued. This reflects that cyber risk is an enduring exposure that is getting continued attention at Senior Management and Board levels, with budgets being approved to increase limits or to purchase as much cyber limit as possible.

The most prevalent corrections applied to cyber programs last year were in the form of capacity reductions, and/or premium and retention increases. Individual insurer capacity for this class of business contracted considerably across 2021, with many markets now capping their participation on an individual risk to $5-$10m regardless of attachment or ventilation. This was particularly evident locally with a decrease in the number of Australian insurers able to write cyber on a primary basis, especially for mid-to-large sized corporations. This lead to the placement of more cyber capacity through London based markets.

Figure 2: More limit decreases as rates rise; limit increases still being pursued

US cyber limits purchasing trends through Q3 2021



Source: Marsh Global Placement & Specialties, Data and Analytics, PlaceMAP Marsh Clients

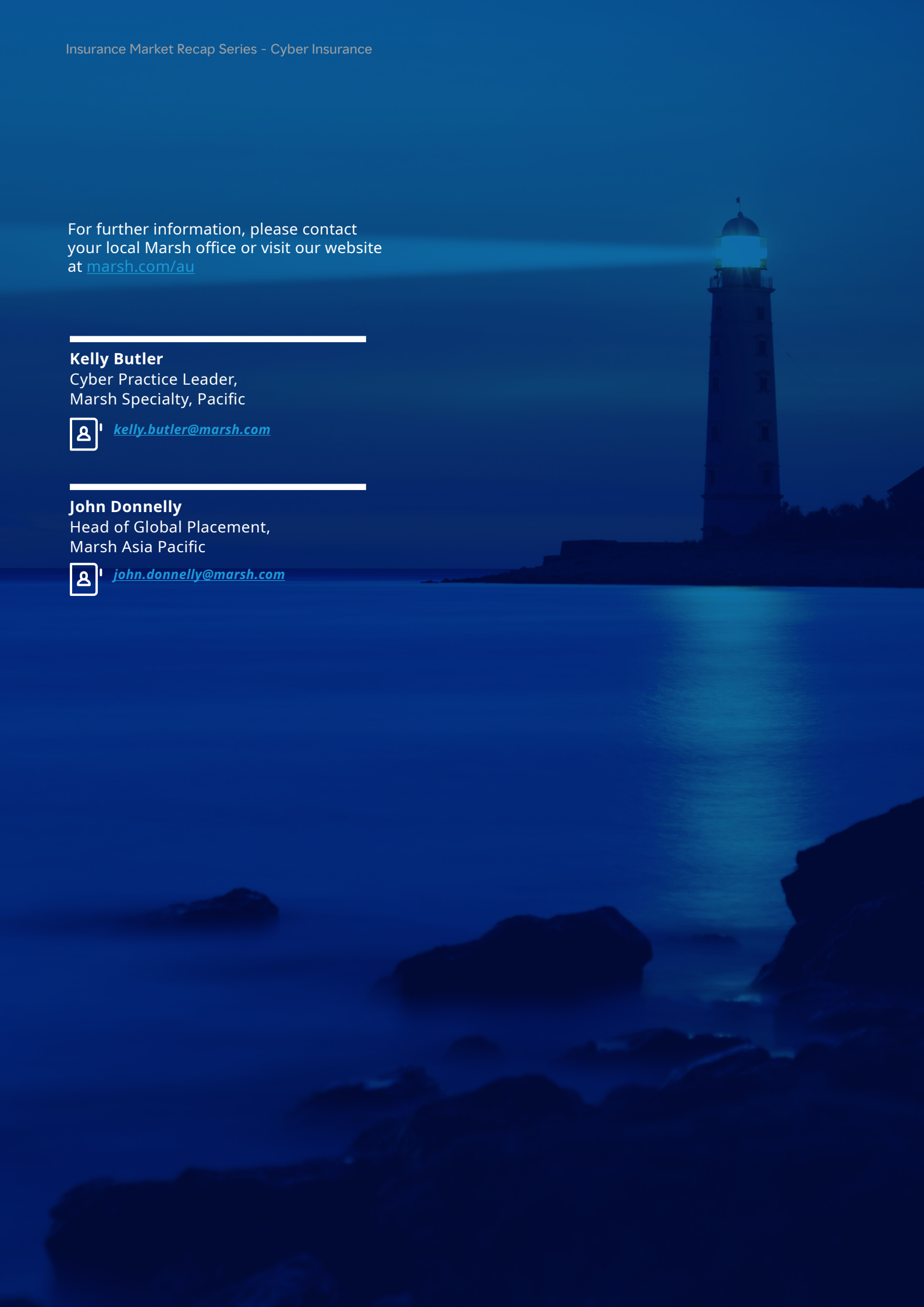
Where to from here?

There is no doubt that 2021 was a tumultuous and challenging period for cyber insurance. The severity of cyber claims exceeded modelling expectations, and threat actors became more ophisticated in their attacks.

Challenges will remain in 2022, but we enter the year with cautious optimism as the corrective actions taken last year to improve portfolio profitability begin to have a material impact. Whilst premium and retention increases, capacity reductions, and coverage scrutiny will remain, we expect that from mid-2022 the extent of these will not be as severe. Material changes will linger through the first and second quarters of 2022 as accounts in this period catch-up with the changes that were applied to placements in the third and fourth quarters of 2021.

One enduring feature will be the heavy underwriting scrutiny over each cyber submission. There is an expectation that businesses are proactive and invest in continually reviewing and bolstering cyber risk maturity. Whilst the specifics will depend on the size of a company or industry of operation, there will be minimum security controls required before insurance quotes are provided. A business that does not meet these requirements will be precluded from transferring cyber risk to the insurance market until such time as improvements are made.

Marsh has a definitive strategy to support upcoming cyber placements. Using proprietary models, our in depth knowledge of cyber risk and security, and our market leading insight into insurer strategy and appetite, we will drive optimal renewal outcomes for our clients.



For further information, please contact your local Marsh office or visit our website at marsh.com/au

Kelly Butler
Cyber Practice Leader,
Marsh Specialty, Pacific

kelly.butler@marsh.com

John Donnelly
Head of Global Placement,
Marsh Asia Pacific

john.donnelly@marsh.com

About Marsh

Marsh is the world's leading insurance broker and risk advisor. With over 45,000 colleagues operating in 130 countries, Marsh serves commercial and individual clients with data-driven risk solutions and advisory services. Marsh is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. With annual revenue nearly $20 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. For more information, visit mmc.com, follow us on LinkedIn and Twitter or subscribe to BRINK.

Disclaimer: Marsh Pty Ltd (ABN 86 004 651 512, AFSL 238983) ("Marsh") arrange the insurance and is not the insurer. This document and any recommendations, analysis, or advice provided by Marsh (collectively, the 'Marsh Analysis') are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. This document contains proprietary, confidential information of Marsh and may not be shared with any third party, including other insurance producers, without Marsh's prior written consent. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, accounting, tax, or legal advice, for which you should consult your own professional advisors. Any modelling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Except as may be set forth in an agreement between you and Marsh, Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party with regard to the Marsh Analysis or to any services provided by a third party to you or Marsh. Marsh makes no representation or warranty concerning the application of policy wordings or the financial condition or solvency of insurers or re-insurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage.

© Copyright 2022 Marsh Pty Ltd. All rights reserved.
LCPA 22/085. S22-0237.