Cyber Insurance Market Insights

Q1, 2021

AON

Overview

In regard to cyber risk, and the insurance market, the landscape has unmistakably changed. Ransomware became an unavoidable topic in Q4 2020, with many insurers forecasting changes to portfolios and possibly coverage as a result of associated losses. Further compounding these challenges were the dual issues of evolving silent cyber[1], and a new cyber incident that may be considered one of the most devastating events in cyber history – SolarWinds.

Whilst there were numerous cyber incidents in 2020, SolarWinds will play a critical role in cyber risk and insurance over the next few years. The theft of investigative tools from a globally recognised cyber security and forensics firm, as part of the SolarWinds compromise, is likely to lead to improved hacking tools in the hands of cyber criminals.

Ransomware attacks have increased in both severity and frequency, as evidenced by Aon's proprietary claims data, with the impacts of the events causing significant concern for insurers. Aon's USA data suggests that ransomware activity has dramatically outpaced data breaches over the trailing four quarters, up over 300% from the end of 2018.[2]

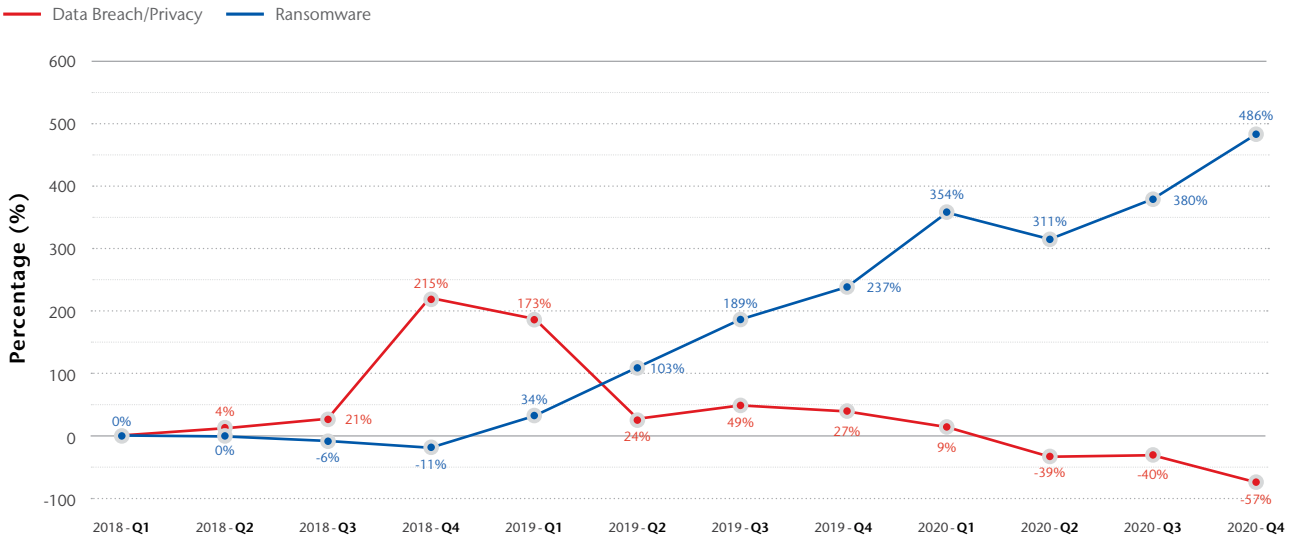
Whilst ransomware has existed for some time, the malware itself has been truly weaponised since its earlier versions. Increased working from home arrangements have provided an opportunity to exploit additional vulnerabilities in organisations' security. This dynamic is shifting at terrible speed, with recent reports emerging of a USD 50m ransomware demand against a hardware/electronics company.[3]

[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] www.aon.com/cyber-solutions/thinking/aons-errors-omission-cyber-insurance-snapshot-a-focused-view-of-2021-risk-insurance-challenges/

[3] www.engadget.com/acer-50-million-ransomware-attack-054534573.html

Data Breach vs Ransomware Attacks, 2018-2020



Source: Risk Based Security, analysis by Aon. Data as of 01/05/2021; Ransomware payment per Coveware Ransomware Report as of 11/14/2020

Silent cyber remains a challenging issue, with cyber exclusions or endorsements being applied to most non-cyber lines of insurance. This topic has been front of mind for a number of years, however there is little consistency between markets or lines of insurance on the exact approach. Further, there is often significant gaps between proposed endorsements/exclusions, and coverage as afforded under most cyber policies, leading to confusion of intention.

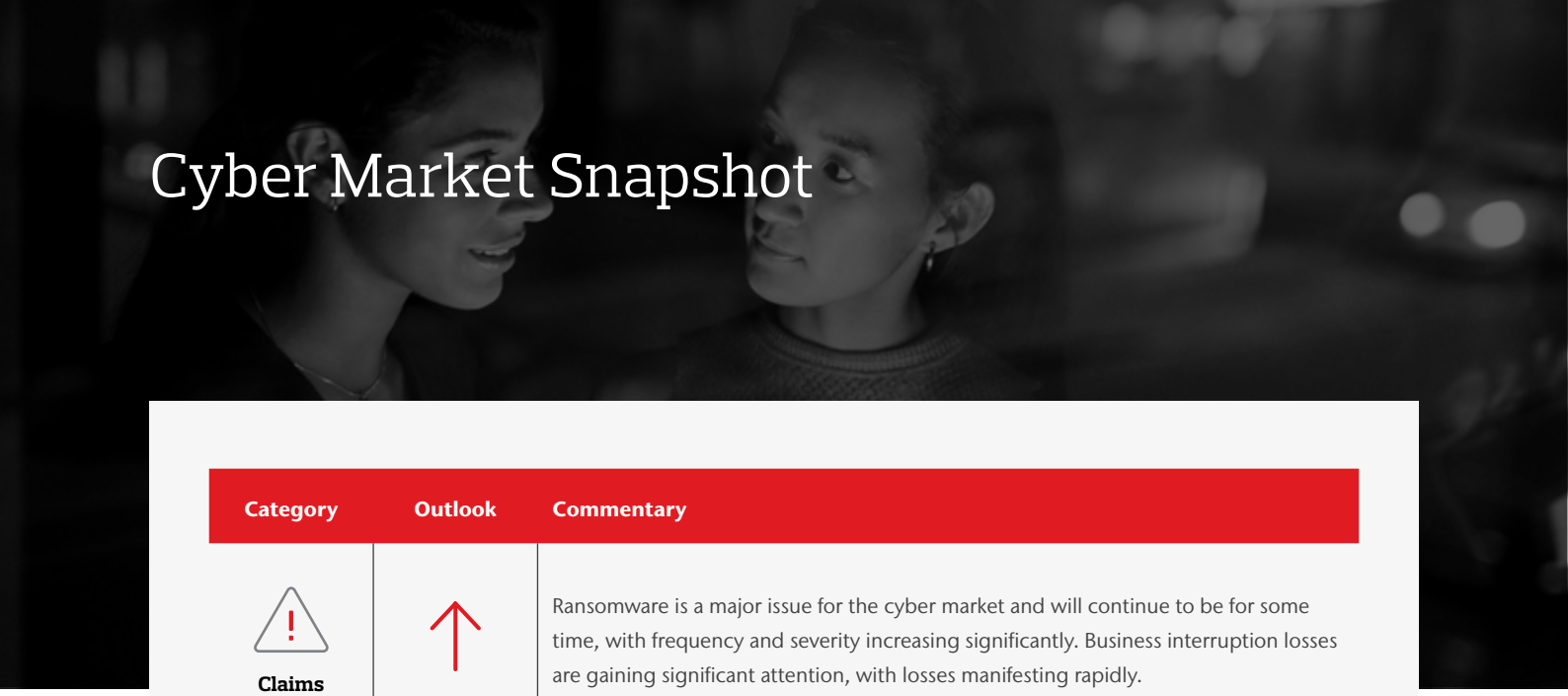
These factors and others, are leading to critical reviews of cyber portfolios, and changes in order to remain viable as a line of insurance are anticipated. This requires an assessment of coverages to ensure they are suitable in the current environment, as well as consideration of appropriate retentions, limits and premiums. Most cyber markets are opting for enhanced underwriting scrutiny, which often includes third-party vendor assessments on externally visible vulnerabilities.

The number of cyber incidents locally has been steadily increasing, with Aon noting a 350%+ increase in matters being managed since the start of 2017, and a minimum 500% increase in average losses over the same period.[4] With many claims/incidents yet to be resolved, this figure will be further impacted. It is worth noting that these are the insured losses, and do not speak to the uninsured losses, which largely go unreported.

The number of high-profile organisations to be impacted by cyber events from 2019 is now staggering, with a growing portion of impacted organisations being non-USA domiciled. This is a rapidly changing landscape, and is expected to continue with recent significant compromises including Acer and Microsoft Exchange, which unearthed multiple zero day vulnerabilities.[5]

[4] Source: Aon proprietary claims data

[5] www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/



Cyber Market Snapshot

Category	Outlook	Commentary
Claims	↑	Ransomware is a major issue for the cyber market and will continue to be for some time, with frequency and severity increasing significantly. Business interruption losses are gaining significant attention, with losses manifesting rapidly.
Pricing	↑	Market conditions are firming with a notable acceleration in Q4 2020. Aon anticipates rate pressure for all organisations, with all insurers suggesting 20% to 40% rate increases for 2021 across insurers portfolio. Excess pricing showed similar, if not greater, increase pressure from Q3 2020 onwards, and is expected to follow into 2021.
Limits	↑	Limit increases were common in 2020 due to a combination of factors including increased risk awareness, increased claims and incidents, silent cyber discussions, and a growing understanding of business interruption costs/expenses.
Retentions	↑	Insurers are seeking to increase retentions. Early insurance adopters may still benefit from reduced retentions; however, expectation is that these will migrate to $500k over a 2-year period. New purchasers however are likely to start at $500k. Time retentions may be increased as well, likely starting at levels of 12 hours, with 24 hours being more common for large risks.
Coverage	↔	Coverage mostly remains consistent, however certain aspects of broadened coverage will be scrutinised more heavily, namely non-IT dependent business interruption and IT dependent business interruption. Ransomware coverage will receive the most scrutiny throughout 2021.
Capacity	↓	Capacity has commenced a slow but steady retraction globally and locally, with some Lloyds markets exiting the space entirely. All insurers are now focused on profitability. With the rapid escalation of losses in 2020, global markets have carefully considered their maximum lines. Many markets are reducing to maximum line sizes of $10m, and in some instances $5m maximum lines.
Underwriting	↑	Insurer attitudes and underwriting practices are adapting to the velocity and impact of the risk environment, which is resulting in increased scrutiny from many markets on overall cyber security posture and in some instances, specific cyber security measures, i.e. multi-factor authentication.

State of the Market

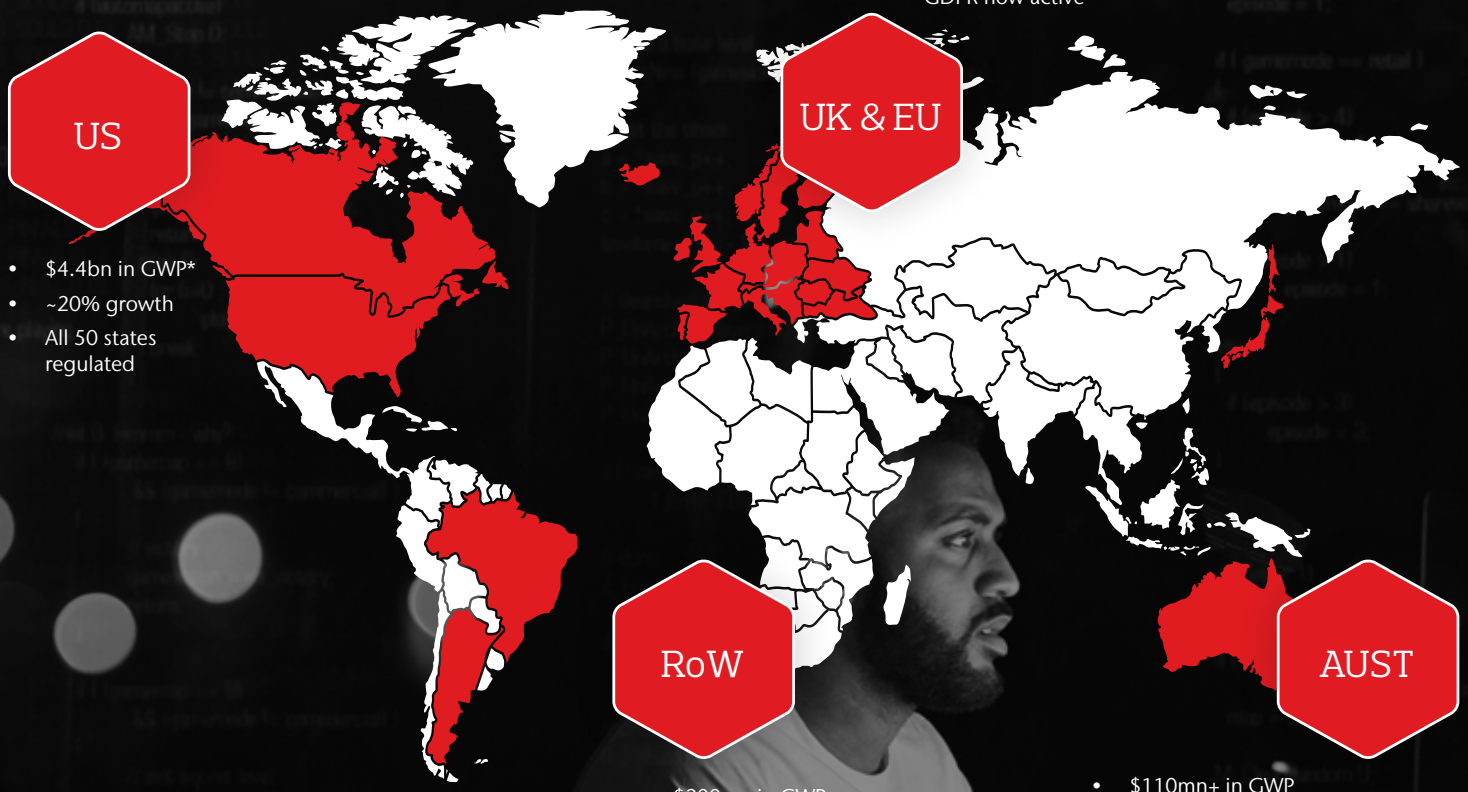
The Australian market is demonstrating transitionary characteristics, similar to those seen in the USA following large losses in the retail and healthcare sectors in past years. A distinguishing characteristic now however is that the impacts are being felt globally. Cyber has historically been a well-adopted line of insurance in the USA. It has been growing steadily internationally, however it has yet to reach similar premium levels. This applies increased international pressure in Australia, where cyber insurance adoption rates are increasing steadily, but are not equivalent to the USA.

This is leading to a localised realignment of limits being deployed by insurers. Some Australian insurers have carefully contracted the amount of capacity they will deploy, and in some instances, insurers have withdrawn from the class of insurance. Internationally it is a similar story, with markets looking to limit the capacity they will deploy, and again in some instances, a number of smaller markets have withdrawn as they have insufficient premium pool to manage a portfolio.

Even more so than premium increase and limit management, markets are increasingly inquisitive of an organisation's security posture. The market has rapidly matured as to sophistication, primarily driven by large losses, and scrutiny of underwriting has increased sharply. Markets are increasingly empowered to walk away from an organisation that cannot adequately explain their security framework and security investment strategy, both historical and future, or to provide terms that are penal or designed to force improved risk management posture.

Aon data reveals a 350% increase in Australian cyber incidents since the start of 2017

Growth of the Cyber Insurance Market



- ~$800mn in GWP
- ~50% growth
- GDPR now active

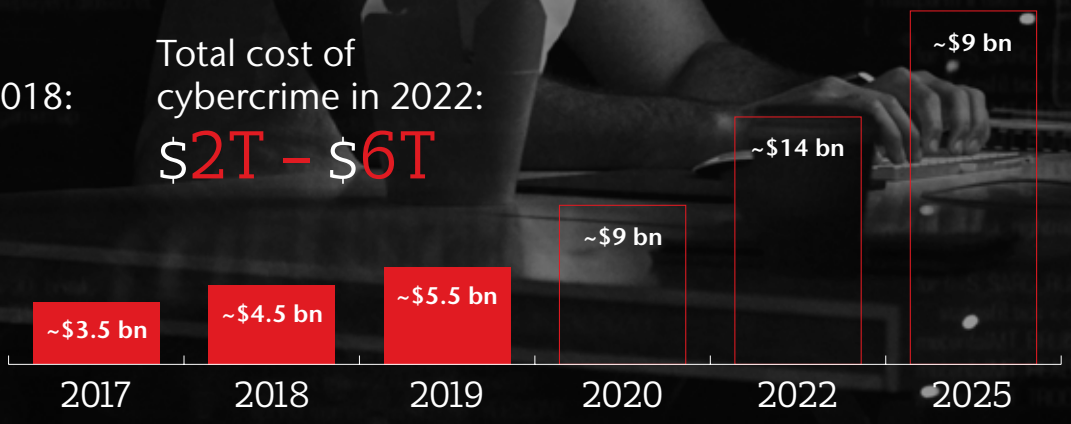
- $4.4bn in GWP*
- ~20% growth
- All 50 states regulated

- ~$200mn in GWP
- GDPR spurring new privacy laws beyond Europe

- $110mn+ in GWP
- MDBN legislation enacted in 2018
- Proposal to broader OAIC powers being considered

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

Ransomware will demand action. We have seen Treasury in the USA tighten controls and raise awareness of payment of ransom demands, including an expansion of sanctions lists to include some known hacking groups.[6] Much will play out over the coming 12 months. We have already seen some markets proactively restrict coverage around this topic for those organisations that cannot convince markets that their security programs adequately address ransomware risks.

Another item of consideration that will become a focus for markets throughout 2021 will be supply chain exposure. Whilst this has been an issue for some time, as insurers start to grapple more fully with ransomware, supply chain exposure will also be scrutinised increasingly. We have seen two large supply chain attacks within the last few months, which will help bring this long-standing issue to the forefront.

Supply chain exposures are critical to cyber markets as it speaks to a potentially unknown aggregation impact. Unlike other classes of insurance, cyber insurance does not have physical boundaries. Other lines of insurance can typically centralise their exposure and model the likely impacts to that exposure. Cyber exposures however can be felt by organisations across the globe, and virtually instantaneously, as has recently been seen with the SolarWinds compromise.

2021 and 2022 are likely to be the first consecutive years of hardening conditions to the cyber market, with the importance of risk selection and underwriting criteria being a focus point for insurers.

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 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 USA, and by 2021 is predicted to be more profitable than the global trade of all major illegal drugs combined.[7]

[6] www.csoonline.com/article/3587108/us-treasury-department-ban-on-ransomware-payments-puts-victims-in-tough-position.html

[7] 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 us

Michael Parrant
Cyber Insurance Practice Leader

t +61 (3) 9211 3485
e michael.j.parrant@aon.com

aon.com.au

CORP20210326