CYBER INSURANCE

MARKET UPDATE 2023

ACP
AUSTBROKERS CYBER PRO

The cyber insurance market has been in a corrective phase over the last 12 to 24 months. This has been driven by many factors, including an increase in claims activity, more rigorous underwriting requirements and a requirement by insurers to address systematic risk exposures on a portfolio basis. We are now entering a more stable market where capacity is re-entering the market and minimum security standards are now required by the industry as a whole. Despite this, insurers are still being cautious and rates are still increasing, albeit at a slower pace than in prior years. One thing has become clear, those organisations who are investing and displaying a strong level of cyber security maturity will achieve much more favourable outcomes in the market moving forward than those that are not.

Claim Trends

Claim trends continue to be mostly in line with prior years, with ransomware events and business email compromise matters leading the way. The last 12 months has seen the emergence of heightened regulatory risk for organisations.

Ransomware Attacks & Resulting Class Actions

Sophisticated ransomware attacks continue to occur, however recent data suggest threat actors are finding it more difficult to extract ransom payments from organisations. According to Covewave, a ransomware incident response firm, 79% of victims paid a ransom in 2019, however in 2022 only 41% of victims paid. This is despite the number of successful ransomware attacks appearing to remain constant.

We are now seeing the reputational harm to organisations and the potential for class action lawsuits following a ransomware attack and/or data breach event, become costlier than the actual ransom demand itself. In the US, class action law suits stemming from cyber events have been a common theme for several years. It now seems Australia is catching up, with lawyers and litigation funders looking into several class actions and confirming their pursuit of Medibank over their large scale data breach in late 2022.

On thing remains constant, ransomware attacks remain extremely costly for organisations and the cyber insurance market, with the cost in relation to investigating the incident, restoring networks and dealing with the regulatory and privacy implications increasing. These events can now also see the organisation's D&O policy at risk, particularity if there has been a lack of oversight around cyber security at a Board level.

Business Email Compromise ('BEC')

Business Email Compromise ('BEC') continues to be a significant threat to many organisations. It continues to be the leading issue for SME organisations. The introduction of Multi Factor Authentication ('MFA') requirements by insurers on cloud-based email networks, such as Office365, has helped increase resilience in this area, however claims are still frequent, as in recent times, threat actors have become more sophisticated with their phishing campaigns and have begun to work around the MFA in place.

Staff education and training remains key, including regular phishing simulation campaigns within organisations. Having clear and concise controls around the transfer of funds to third parties, including call back procedures is another key risk management function that organisations should implement.

Heightened Regulatory Risk

The increase in regulatory risk for organisations around cyber security has been evident over the last 12 months. This is due to regulators increasing their focus on cyber resiliency and understanding the increasing public expectation that organisations holding personal information of their customers, must be taking reasonable steps to secure that information.

ASIC's recent Corporate Plan for 2022-26 lists one of its top three key priorities as cyber/technology and operational resiliency. It has shown a willingness to pursue organisations who are not addressing cyber security and taking reasonable steps and investments in this space, as was evidenced in their case against RI Advice.

Changes to Australia's Privacy Act are also underway, with some of the key reforms likely to be around:

- Amendments to increase the maximum penalties for organisations with serious or repeated privacy breaches from the current $2.2m to whichever is the greater of the following:
    - $50 million;
    - three times the value of any benefit obtained through the misuse of the information (if a court can determine this);
    - or if the value of benefit obtained cannot be determined, 30% of a company's adjusted turnover in the relevant period.
- An increase in information gathering powers for the Office of the Australian Information Commissioner ('OAIC') in relation to suspected eligible data breaches, including serving written notices and requesting the production of documents.

The above has the ability to not only increase the risk and claims costs to organisations, but it may have implications on the third party liability areas of a cyber insurance policy.

Current Market Dynamics

There are various dynamics driving the market at this point in time.

Demand for Cyber Insurance is Increasing

With the claim trends noted above gaining significant media attention, along with organisations continuing to increase their reliance on technology, demand for cyber insurance continues to increase as organisations continue to look for a mechanism of risk transfer regarding the residual risk exposure that exist within all organisations.

Discussions with risk advisors (such as insurance brokers) and Boards continues to increase, with the ability to procure sufficient cyber insurance coverage heavily dependent on the risk controls and maturity of an organisation and the ability for a specialist cyber insurance broker to have meaningful conversations with the insurance market.

Minimum Security Controls a Standard Requirement

More rigorous underwriting from insurers has ensured those organisations looking to procure and/or renew cyber insurance programs are required to display a strong control environment. This has led to improved cyber hygiene amongst organisations. Minimum security standards such as Multi Factor Authentication ('MFA') on remote access into networks and cloud based email accounts, strong controls around privileged access, patch management policies, the implementation of EDR solutions, cyber security awareness training for all staff, strong backup protocols and testing, along with detailed and tested incident response and business continuity plans addressing ransomware incidents are now expected by the insurance market.

As cyber risk continues to evolve, so will the underwriting and controls standards expected by insurers. This positive development in the market ensures those organisations investing in their cyber security posture are now clearly achieving better outcomes when it comes to coverage and premiums, as more insurers are willing to provide competitive terms on these accounts. Those organisations who are not will continue to achieve poor outcomes and, in many instances, will not be able to obtain the cyber insurance they wish to acquire.

Additional Capacity within the Market

We have recently seen an increase in capacity within the market from both local insurers and underwriting agencies, along with Lloyd's of London syndicates. Some markets paused on writing new cyber business whilst they implemented strategies to address systematic risk exposures and reviewed their portfolios as a whole. With thorough underwriting now taking place and an expectation around increased cyber hygiene amongst organisations, along with more attractive rates, insurers, for the most part, are now looking to grow their cyber portfolios once again.

Capacity deployment remains controlled; however some insurers and agencies are now willing to deploy up to $10m of capacity if they believe the risk is attractive. This additional capacity is now starting to create competition within the market again, ensuring those organisations displaying strong controls and processes are benefiting, whether that be first time purchasers or those organisations renewing their program.

Coverage Continues to be Reviewed

Even with new capacity entering the market and an increase in cyber hygiene amongst insured organisations, insurers continue to grapple with elements of coverage within their cyber insurance policies. Addressing systematic risk exposures continues to be a concern and priority for all insurers, especially when those insurers are trying to purchase reinsurance.

Lloyd's and other carriers continue to propose and amend exclusionary language to address cyber operations between nation states via war type exclusions. Silent cyber continues to be a concern for insurers, with the majority of insurers now being clear that cyber risk needs to be addressed via standalone cyber insurance policies. Legal cases have begun to emerge which also confirm this position, which in turn continues to drive demand for stand alone cyber insurance programs.

Premiums Rising but Beginning to Stabilise

Whilst premiums continue to rise, there has been a slowdown, compared to the peak at the beginning of last year. The start of 2022 saw premium increases peak at around 100% on a global basis, whilst towards the end of 2022, globally premium increases were around 53%. Pricing in Australia remained quite challenging throughout 2022 with a lack of capacity within the market, leaving organisations with few options to consider.

As noted previously, with additional capacity now coming into the market, premiums continue to stabilise which is a good thing for organisations. We see this trend continuing throughout 2023 and believe those organisations with strong cyber hygiene will attract competition amongst insurers, meaning more favourable premiums and conditions can be achieved moving forward.