CYBER INSURANCE

MARKET UPDATE 2022

ACP

AUSTBROKERS CYBER PRO

The cyber insurance market continues to go through significant changes and an acceleration of hard market conditions has been seen within the last 12 months. The claims activity in this area continues to be significant for insurers, driven by ransomware events and business email compromise issues. Insurers and underwriting agencies are taking corrective action across their portfolios, with large premium and deductible increases, reductions in capacity and a tightening of coverage. The requirement around minimum cyber security standards has accelerated over the last 6 months, with most insurers and underwriting agencies now requiring a set of minimum cyber security standards to be in place for organisations to procure or maintain their cyber insurance policy.

Claim Trends

Ransomware Attacks

Sophisticated ransomware attacks continue to occur. These attacks continue to be concerning to organisations. Threat actors are continuing to take data and threatening to release it publicly if ransoms are not paid. There has been an uptick in recent times of smaller organisations being subject to ransomware events, with smaller ransom demands being requested, which is likely due to threat actors wanting to create little fuss and stay away from larger and publicly known organisations, given the backlash that has occurred due to some high-profile attacks in the past, including the Colonial Pipeline incident.

The recovery process around ransomware events continues to be problematic for organisations, with those organisations who have strong cyber security processes, including backups, far more likely to recover in a timely manner.

Business Email Compromise (‘BEC’)

Business Email Compromise (‘BEC’) continues to be a significant threat to many organisations here in Australia and around the globe. Despite a slight decrease in these incidents, it is still the most common cyber incident we see for SME clients. 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, and organisations should continue to work closely with their IT personnel/ providers on ensuring they are correctly securing their email environment.

Software Supply Chain Events

The emergence of software supply chain vulnerabilities has caused many insurers to carefully think about their aggregation exposures and impose additional underwriting questions and policy conditions. The existence of vulnerabilities within software (some of a zero-day nature) is a major concern insurers are beginning to tackle as they look to control their exposures to such widespread events. The concern for insurers is that if hundreds of thousands of their clients are using a piece of software with a vulnerability and a threat actor takes advantage of such vulnerability, the insurer could get thousands of claims all at once, which would put the viability of their cyber portfolio at significant risk. In recent times, incidents like Solar Winds, Microsoft Exchange, Pulse VPN and Log4j have put insurers on notice. At this stage, the claims activity regarding these software supply chain events has not been significant, however as more organisations around the world purchase cyber insurance, there is no doubt claims activity in this area will continue to be a concern for insurers.

Response from Insurers

Minimum Cyber Security Standards

Insurers and underwriting agencies have accelerated their requirements for organisations to have a minimum set of cyber security standards in place to procure or maintain cyber insurance coverage. There is now little tolerance in the market for organisations who are not taking their cyber security posture seriously. Such organisations will either (a) not be able to procure or maintain their cyber insurance policy or (b) have significant restrictions, such as ransomware exclusions placed on their cyber insurance policy. ACP have recently put together a Cyber Security Standards Checklist and a summary of those standards is outlined below.

- Multi Factor Authentication ('MFA') is expected on all remote access into networks (including the use of O365 and other cloud-based platforms).
- Strong controls are expected in relation to internal privileged access accounts, including a Privileged Access Management ('PAM') tool, the principal of least privilege and the deployment of MFA on those accounts.
- A patch management policy is expected to be in place outlining the patching credence of the organisation.
- A strong Incident Response, Business Continuity and/or Disaster Recovery plan, which deals with and addresses downtime of IT networks due to a cyber incident is required. Back Ups need to be tested on at least an annual basis for integrity. Back ups need to be taken offline and encrypted.
- An Endpoint Detection & Response ('EDR') tool should be implemented across all endpoints within the organisation, including workstations, laptops, servers etc.
- Vulnerability scans and penetration test should be conducted on at least an annual basis by a third-party specialist.
- End of Life/Unsupported systems and software should be isolated from the network and guidance around plans to decommission and upgrade such systems and software should be provided.
- Strong controls are expected in relation to protecting Personally Identifiable Information ('PII') within the IT environment. The use of a Security Information & Event Management ('SIEM') tool should be considered.
- Cyber security awareness training should be implemented within the organisation. This training should include phishing simulation exercises.

Premiums & Deductibles

Premiums have increased drastically over the past 6 – 12 months. In the last quarter (Q1 2022), rate increases of 110% in the US and 102% in the UK were experienced. The UK rate increases have a flow on effect to the Australian market, given most underwriting agencies operating in the cyber market in Australia are backed by Lloyd's of London capacity. In the Australian market, premium increases of between 25% - 50% are the norm in the SME space, whilst corporate programs are seeing significant premium increases of between 50% - 100%, in some cases, increases were higher.

To offset some of the increases, organisations have been opting for higher deductibles on their cyber insurance programs, however in many cases, higher deductibles have also been forced on to organisations as the market pushes to increase self-insured retentions.

Capacity & Coverage

Capacity in the cyber market remains far more constrained than previously. Almost all insurers and underwriting agencies are now deploying no more than $5m on a single risk with a view of bringing down their overall cyber aggregation. Those programs where a $10m limit is deployed by an insurer are seeing that limit halved and the premium in many cases greater than what it was previously. Capacity control is here to stay on cyber with new capacity in the future likely to come from new market entrants, not from current market participants.

Coverage is being looked at closely by insurers and underwriting agencies alike. Major market participants continue to deploy ransomware endorsements that either sub limit and/or enact co insurance requirements on ransomware claims.

A clear market standard is MFA on remote access into networks and many insurers will now not provide terms without this being in place, or if they do, exclusions in relation to ransomware claims will be imposed on policies. Insurers and underwriting agencies continue to ask additional questions in relation to supply chain vulnerabilities and impose exclusions if organisations cannot demonstrate they have addressed these issues. End of Life software/systems also continue to be excluded, pushing clients to bring forward their plans to upgrade elements of their network.

On a final note, the inclusion of requirements within cyber policies is beginning to emerge. For example, some insurers in the market now have conditions built into their policies (either with their wordings or via endorsement) in relation to certain security requirements, with a particular focus on patching credence. Failure to adhere to such requirements can void a cyber insurance policy or reduce areas of coverage under the policy.