CYBER INSURANCE

MARKET UPDATE 2021

ACP
AUSTBROKERS CYBER PRO

The cyber insurance market is currently going through some significant changes due to a large uptick in claims activity in the last 12 months. Some of this claims activity can be attributed to the shift of workforces globally to remote working environments due to the onset of the COVID19 pandemic. Large ransomware events continue to dominate the claims environment, which is forcing insurers to review their cyber insurance portfolios and make adjustments to premiums, excesses, coverage and underwriting guidelines.

Claim Trends

Ransomware Attacks

Sophisticated ransomware attacks continue to occur and do not look like stopping anytime soon. There have been some very large attacks against large global companies which have crippled their IT networks and ability to operate efficiently. Australia is not immune to these ransomware events, with many Australian companies also being affected. Threat actors are changing the game by *taking an organisation's data* and threatening to release it publicly if ransoms are not paid. The recovery process to get systems back online can take weeks (sometimes months) which can result in large costs around data recovery/restoration and business income loss. We are starting to see larger organisations in Australia *scale up* their cyber insurance programs/limits, as they are beginning to understand the risks associated with the loss of their IT networks for a prolonged period of time.

Business Email Compromise ('BEC')

Business Email Compromise ('BEC') continues to be a significant threat to many organisations here in Australia and around the globe. This is the most common cyber incident we see for SME clients. These breaches can be costly to insurers due to the frequency and potential requirements that organisations must adhere to under the Privacy Act here in Australia, including notification to the Office of the Australian Information Commissioner ('OAIC') and affected individuals if an *eligible data* breach is suspected.

Claims Costs to Insurers

The costs to cyber insurers continues to be mostly in relation to the *first party* areas of a cyber insurance policy. The real benefit of a cyber insurance policy is the assistance the policy provides (in terms of costs and vendors) in assisting an organisation get their IT systems back up and running following a cyber event.

The majority of costs at claim time fall within the following two sections of a cyber insurance policy:

1. *Data Recovery Costs* – these costs are incurred to assist the Insured in getting their systems back up and running and online as soon as possible. The costs can be significant depending on the complexity of the cyber event, including whether backups have also been encrypted, and/or corporate or personal data has been exfiltrated by the hackers.

2. *Business Interruption Costs* – these costs are incurred due to the loss of business income experienced by an organisation due to their IT systems being offline. These costs can add up quickly, especially for those organisations who rely on operational technology within their business processes, i.e. transportation and manufacturing companies.

At this point in time, costs around third party claims in relation to data breaches are not overly likely in Australia. Despite this, class actions law suits and strong regulatory action following data breaches in Europe (through GDPR) and in the US is a common theme. It is highly likely in the future, Australian businesses will start to experience such third party claims, including regulatory actions. This will be a further concern for cyber insurers who will begin to see third party liability areas of their cyber insurance policies hit with claims activity.

Response from Insurers

Many insurers in the market, both locally and in London, have responded swiftly and strongly to protect their cyber insurance portfolios and ensure profitability is possible moving forward. Their responses have centred around premium and excess increases, tighter underwriting controls, including minimum IT security requirements, and the introduction of exclusions/reductions in coverage and capacity on cyber insurance programs.

Premiums & Excesses

Insurers are moving premiums in an upwards direction. Premium increases in the SME space are ranging from anywhere between 15% - 40%, whilst in the corporate space, increases in excess of 50%-60% are not uncommon. In higher risk industries or under-priced programs, premium increases can be much higher.

Insurers are also now demanding organisations take more *skin in the game* and are increasing their excesses or imposing higher excesses if an Insured does not have correct risk management processes in place, such as MFA on their network, or regular cyber training deployed within their organisation. Insurers are using such tactics to encourage organisations to implement tighter controls within their IT environment and on some occasions are then able to review excess structures again either during the policy period or at renewal time, once organisations have implemented stronger controls.

Tighter Underwriting Controls

As mentioned above, insurers are now demanding stronger controls and minimum IT security standards for organisations in order to provide terms or renew existing business. The days of *lax* underwriting are over, with insurers now focusing on how an organisation secures their network. Some areas insurers are looking closely at within their underwriting process are as follows:

- MFA deployment in relation to remote access (RDP/Office 365) into an organisation's IT network.
- Diligent and robust processes in relation to data backups and storage, including an emphasis on data segregation and ensuring offline data storage.
- Ensuring organisations have *tried and tested* business continuity or disaster recovery plans with clear Recovery Time Objectives ('RTO')
- The deployment of Endpoint Protection within the IT network and across devices.
- Regular and comprehensive patching policies and procedures.
- Regular cyber security awareness training being deployed across an organisation.

Along with the above, insurers are also looking closely at legacy systems which are no longer provided with technical support from vendors, i.e. Windows 7 and also focusing closely on controls and process in place for organisations to deal with ransomware events, including the requirement from some insurers for *ransomware addendums* to be completed by organisations as part of the underwriting process.

Reductions in Capacity & Coverage

Insurers are now deploying capacity in a very cautious manner. The vast majority of insurers are controlling their capacity deployment to $10m on any single risk, with some insurers, particularity in London only providing $5m limits per risk. The inclusion of sub limits in relation to *contingent* Business Interruption expenses is now becoming more common, along with sub limits or co insurance arrangements in relation to ransomware events.

Depending on the security posture of an organisation, insurers are also limiting coverage in certain areas of their cyber insurance policies to try and contain their losses. Common exclusions include, but are not limited to:

- Unencrypted portable media device exclusions.
- Loss of Technical Support exclusions around legacy systems and software.
- Exclusions in relation to known vulnerabilities and/or large global supply chain type breaches, including Solar Winds.
- Coverage *carve outs* for Shared or Dependent computer networks (i.e. those networks managed by IT service providers).
- Exclusions and limit reductions/co insurances in relation to ransomware events, which sit across all areas of the policy.

It is now more important than ever to work closely with the insurer(s) and the Insured in ensuring the best possible cyber insurance coverage can be provided under their cyber insurance program, including highlighting any exclusions placed on coverage and how such exclusions may impact the organisation's cyber insurance program.