INSIGHTS

It's complicated: The challenges of obtaining cyber insurance (and what to do about it)

Publications and reports 09 February 2023

The threat of malicious actors breaching commercial firms' and Government entities' cyber defences continues to escalate. Banks, investment funds and

insurance companies are particularly attractive targets because of the rich rewards on offer, so much so that the financial sector now ranks second only to health organisations for damaging data breaches.

The head of ANZ Bank's institutional bank, Mark Whelan, considers cyber risk the single biggest threat facing the banking industry today. And in its annual cyber risk report for 2022, our Australian associate firm, MinterEllison noted that Australian organisations reported a 15% increase is ransomware events in the 2020–21 financial year compared with the previous year.

With cyber crimes increasing in number, sophistication, and severity, it is more important than ever for businesses and other organisations to protect themselves from cyber attacks and the resultant business losses and liabilities to third parties. This involves implementing IT security systems and procedures, ensuring that staff are appropriately trained, and taking out appropriate cyber insurance.

Cyber insurance poses increasingly complex challenges for insurers, brokers, and insureds. Insurers rely on predictability to accurately assess risk and set appropriate premiums. In the case of cyber crime, however, they are chasing a moving target. Meanwhile, insurers can afford to be more selective, as demand for cyber cover increases while insurer capacity and appetite for cyber risks reduces. Cyber insurance is increasing in cost and reducing in cover.

Key risks and strategies

We recently hosted a Cyber Risk breakfast at which leading professionals from the legal (MinterEllisonRuddWatts), insurance (AIG), insurance broking (Aon) and IT security (Datacom) industries shared insights on cyber risks and cyber insurance in New Zealand.

The key take-outs from that event included the following:

New Zealand is a soft target. Our small size and geographical isolation lulls us into a false sense of security. This is wrong: the nature of cybercrime renders a potential victim's location irrelevant.

Ransomware claims increased 150% from 2018 to 2020 (although the number is beginning to plateau) and by 2021 they comprised one in every five claims. They are increasingly sophisticated, with bad actors now targeting their attacks for maximum damage and effect. Losses include ransom costs, event management costs (such as IT costs), network interruption losses, regulatory actions and customer claims.

The two best ways to address cyber risk are mitigation and insurance.

Good IT 'hygiene' and doing the basics well – such as prompt installation of patches and quick responses to cyber events – are critical.

Remote working increases risk.

Many organisations run legacy systems with inadequate security. Insurers are asking increasingly detailed questions about customers' IT systems and they will decline to offer cyber cover to those with inadequate security. As a result, cyber insurance cover is becoming a mark of quality for organisations as insurers will only cover firms that have good security technology and practices.

Losses from cyber crimes include the victim's own loss and damage (operations are halted, money may be stolen), liability to customers and third parties (whose data may be released or misused), and regulatory action and

fines. Victims should make no admissions, take prompt steps to recover systems, involve insurers at the outset and take appropriate advice.

Threats have been increasing, although their number and severity may be plateauing

There has been no let-up in the onslaught of cyber crime. In 2022, Forbes magazine reported an increase in weekly attempted cyber attacks targeting corporate networks in 2021, up 50% on the previous year. Around the same time, the FBI's Internet Crime Complaint Centre issued a public service announcement reporting a 65% increase in identified global losses between July 2019 and December 2021.

The New Zealand Government's Budget for 2022 provided approximately $50 million in additional funding over four years for the GCSB to combat cybercrime and engage in counter terrorism activity. The move reflects concerns around increased frequency and severity of cyber attacks, and aims to protect information services increasingly at risk of cybercrime.

More recently, however, anecdotal evidence from London insurers has indicated that, while not decreasing, the number of cyber crime related claims is appearing to have plateaued. While the ingenuity of criminal actors continues to develop, there is also an increasing sophistication among potential targets.

Cyber insurance is increasingly challenging to obtain

Insurers are responding to the rising risks and costs of cyber events with increasingly detailed assessments of insureds' IT systems, as well as by reducing cover limits and increasing premiums. One major New Zealand insurer has dealt with this additional complexity by introducing a 'smart' cyber questionnaire in which an insured's answers to the initial questions trigger different or additional questions, depending upon the responses. Other New Zealand insurers have reduced limits significantly or have withdrawn cover altogether. Large firms, such as those with revenue over $100m, are facing increased scrutiny as they present a greater perceived risk.

The complexity of insurers' questionnaires, and their importance, means that IT departments must be well prepared and resourced to answer them. This should be done in advance of the cyber insurance renewal date, as the time commitment is significant, and answers often need to be drawn from different sources. IT departments may realise as they work through the questions pre-emptively that their answers will not satisfy the insurers, so it may be necessary to take remedial steps ahead of time so that a better response can be given.

An additional challenge is that whereas previously insurers might have accepted insureds' responses uncritically, many now test and challenge them. Insurers will often share reports with the insured, and sometimes insureds and their brokers will need to challenge aspects of an insurer's report that may not tell the full story.

A key lesson for brokers and insureds is that 'wrong' answers to questions asked by insurers may have significant effects upon their willingness to offer or renew cyber cover. It is crucial that insureds provide a full explanation of any responses that might not tell the full story. For instance, insurers expect to see multi-factor authentication as a core requirement for access to an insured's system. This means that any circumstances in which multi-factor authentication may not be used, such as where there are other security systems in effect, will need to be explained.

Brokers and insureds need to prepare for their renewals with a full appreciation of the time and work that is likely to be required to present a compelling proposition to a cyber insurer. Insureds will also need to be prepared to consider reductions in cover or moving to different insurers as capacity and limits change.

Insurers, for their part, will need to continue monitoring claims closely and adapting quickly as bad actors change their approaches and the threat landscape develops. Cyber insurers will increasingly need to provide a proactive,

advisory service to assist brokers and insureds to understand what their requirements will be and enable insureds to satisfy their expectations, rather than confining their role to a reactive response.

Insurers' reliability and consistency is increasingly valued

The cyber insurance market is volatile. Some insurers that were cyber market leaders in New Zealand in 2020 had reduced capacity in 2021, while others offered new capacity to help meet the resulting demand. Brokers report that many customers were obliged to place cover with new insurers. This further added to the burden faced by insureds' IT departments as they were asked to respond to multiple insurer questionnaires.

Because of this, insureds will increasingly value stability and consistency in their cyber insurers and may prioritise those characteristics over price and cover limits.

Cyber insurance continues to offer real value

While cyber insurance is increasingly challenging to obtain, brokers report that it continues to benefit insureds. Perhaps because of the care taken when it is arranged, it features a relatively high claim acceptance rate compared with other types of insurance.

Cyber insurance also remains one of the few insurance products that assists insureds to prevent claims. Insurance assessments are often valuable tools to identify security weaknesses and remedy them, as insurers often have up to date knowledge of the latest risks. Cyber insurance discussions can therefore benefit insureds by assisting them to improve their systems and remove vulnerabilities.

There is also the additional benefit that cyber insurance provides a badge of quality, as it demonstrates that an insurer has assessed the insured as a good risk. For professional services firms in particular, whose own customers are increasingly demanding reassurance as to their cyber defences, this is likely to be increasingly important.

Related material

READ THE FORECAST ↓

Key contacts

Speak with one of our experts.