www.al.nz | lawyers@al.nz

26 June 2020

Cyber risk: a changing landscape

It has been reported that the latest ransomware attack against the brewer, Lion Australia, came with a demand for US$800,000. Is the recent spate of cyber attacks in Australia a cause for concern here in NZ? And how well prepared are businesses for this threat?

Business critical risk or headache for the IT department?

Many businesses with business interruption policies will have dusted them off only to learn that either cover was not triggered (due to there being no "physical damage"), or exclusions for infectious diseases and the like, meant there was no policy response. So whilst ambivalence about the utility of insurance "add-ons" might be perfectly understandable, it is unlikely to be the best time to take a complacent approach.

The better view is that the considerable time and effort businesses have invested in understanding the risks they face, should not be wasted. Rather, the intelligence gathered should be directed at reviewing whether existing insurance arrangements remain appropriate for the new normal. In particular, whether previous assessments of business risk from a cyber perspective, should now be paid closer attention.

If recent cyber attacks across the Tasman at the Australian brewer are any reflection of an increased risk environment here in New Zealand, then we might expect to see more domestic examples. Just recently, CERT NZ (the government body that provides assistance to businesses that have been hacked) has warned that hackers are targeting remote workers using Citrix to access their systems.

Certainly, against a backdrop of increased appetite for flexible working, there will be additional security demands on IT systems which potentially were already outdated or unfit for purpose.

There is also the regulatory environment to consider, such as new privacy legislation due later this year (where the stated purpose of the new Privacy Bill is "to promote people's confidence that their personal information is secure and will be treated properly"). The Privacy Act 2020 will introduce a privacy breach notification regime and will allow the Human Rights Review Tribunal to award up to $350,000 to each member of a class action.

Against this backdrop it is estimated that less than 10% of businesses here in New Zealand have a cyber insurance policy. There are undoubtedly a host of reasons for this relatively low uptake, but either way it does raise questions as to how well prepared (and resourced) New Zealand businesses are in the face of this threat.

We suspect the principal reasons for the relatively low uptake of cyber policies concern perceived cost/benefit, mixed with a general lack of understanding around what cover these policies actually provide. It is also likely that erroneous assumptions regarding the extent of cover provided by existing liability policies plays a part. These factors combined with an outdated view that cyber risk is an operational matter reserved to the IT department, rather than a business critical issue, perhaps also explain some of the disconnect.

It is therefore helpful to consider what costs can typically be covered by a cyber policy. Whether the cyber cover is standalone or bolted on to existing policies, it is obviously critical that it is tailored appropriately for the business' specific needs, and also that there are no gaps and/or unintended conflicts with existing policies.

Cyber risk: a changing landscape
(Continued)

What cyber insurance covers

As with all insurances, cyber insurance policies have different terms and levels of coverage:

First party cover – damage caused to your business

First party cover is usually for incidents occurring or losses discovered during the policy period and tends to include:

- breach costs – for example, costs of getting experts to investigate the cause and scale of the breach
- restoration costs – for example, costs of repairing damage to software and data caused by a hacker, such as removing malware
- response management – for example, getting expert advice to help develop communication strategies to limit reputational damage
- business interruption – for example, paying back fee income that would have been earned
- costs relating to cyber threats – for example, paying ransom costs

Third party cover – damage caused to clients and others

Third party cover tends to be triggered by claims made during the policy period and includes:

- privacy protection – defence costs and settlements following legal action or investigation after a data breach, invasion of privacy or breach of confidentiality
- media content liability – defence costs and settlements following legal action as a result of content on the firm's website or social media

As will be evident from the above, the insurance premium for a cyber insurance policy is likely to be modest compared to the potential costs of responding to a cyber breach, and particularly for smaller business, those costs could potentially be crippling. The reputational and business interruption issues can also be particularly difficult to quantify and manage

Want to know more?

If you would like further information or advice in relation to insurance related issues, please do not hesitate to contact our insurance team.