Cyber Threats: Australia's Reality

BOARD DISCUSSION

Spotlight on Cyber Threats

Australian businesses face a significant risk of cyber events.

To ensure the best outcome in the event of a claim, businesses must understand their cyber risk exposures and how the addition of a cyber policy might interact with their existing insurances.

Australian organisations have become a frequent victim of cyber events. Media attention, traditionally focused on breaches faced by overseas entities, has quickly turned to detailing the regular occurrence of cyber events closer to home.

"A range of Australian organisations have been affected, cutting across many industries. Although certain sectors, like healthcare make more likely targets, we have seen breaches across government, financial services, legal firms, logistics, utilities, education, retail, resources and many others," says Kelly Butler, Cyber Leader at Marsh.

In addition to the reputational damage from negative headlines, cyber events result in real and significant costs to Australian businesses in the form of data breach notifications, third party liabilities and ransomware. The growing risk of cyber events could cost the Australian economy up to US$16 billion over the next decade, according to *Lloyd's City Risk Index 2015-2025*.[1] Based on data from the *Beazley Breach Insights Report (October 2016)*, ransomware attacks in 2016 is likely to quadruple compared to 2015.[2]

WHAT ARE SOME RECENT ATTACKS IN AUSTRALIA?

Fake emails masquerading as legitimate correspondence from Australian energy providers have been circulating and misleading customers into believing they owe money for an outstanding bill. These phishing scams capitalise on recent severe weather events and bait the "hook" by suggesting that customers affected by recent weather damage could seek payment relief by clicking on the email link. To date, more than 10,000 Australians have fallen victim to this scam[3], which delivers malware that has the potential of locking the system or computer.

As the world becomes increasingly digitised, even the traditional "snail mail" provider, Australia Post, is being targeted. The company has seen its customers receive fake requests for payment of undelivered parcels, phishing emails with fake login sites requesting for personal information, and malware attachments masked as print labels to redeem packages.[4] The seemingly ordinary scenarios created by scammers mean that many unsuspecting customers have been (and may continue to be) duped.

Every company thinks their systems and data are secure. That is, until something happens. Human error is a risk that can never be completely eliminated. The Australian Red Cross Blood Service was recently caught up in one of the country's largest data breaches. Some 550,000 donors' highly sensitive personal information was leaked online after a back-up copy of the data was inadvertently stored in an insecure environment by a contractor.[5] A classic case of human error, this was a sound reminder that cyber risks can arise from both first or third parties, intentional or non-intentional.

1 www.abc.net.au/news/2016-11-04/sydney-ranks-world's-12th-in-cyber-attack-exposure/7994806, http://www.lloyds.com/cityriskindex/
2 www.beazley.com/beazley_projects_ransomware_attacks_to_quadruple_in_2016.html
3 www.scamsfakes.com/category/phishing-scams/
4 http://auspost.com.au/about-us/scam-alerts.html
5 www.donateblood.com.au/media/news/blood-service-apologises-donor-data-leak

HOW DOES CYBER INSURANCE RESPOND?

"Although we've seen several examples of recent attacks in Australia, it's not always easy to understand how, or if, an insurance policy responds," explains Butler.

"Claims are assessed on a case by case basis, and some can get quite complicated depending on the loss scenario and the type of insurance policies a company has in place. We have seen cyber insurance respond to data breach notification costs, reputational costs, cyber extortion ransom demands, and third party liability cover for claims alleging third parties' information was compromised."

Lloyd's has estimated a 168-fold increase in the amount of cyber insurance being purchased in Australia over the last two years.[6] As the market for cyber insurance grows and matures in Australia, an increasing number of cyber insurance claim payments have been observed.

"We are seeing more and more cyber related claims being paid by insurers. When structured correctly, cyber insurance can be an effective risk transfer option for businesses," says Butler.

HOW SHOULD YOU EVALUATE A CYBER POLICY?

Cyber insurance is not a one-size-fits-all solution. The type and amount of cover purchased are driven by a number of factors including an organisation's industry, maturity of cyber-risk management, business continuity planning and overall attitude and willingness to accept risk.

As with all insurance, cyber policies are not created equally. In order to ensure the best outcome in the event of a claim, organisations must understand their own risk exposures and the cover they are purchasing. In many cases, partial cover may exist under current insurance policies, so companies need to have a clear understanding of how the addition of a cyber policy might interact with their existing insurances to avoid any unnecessary overlaps.

"One way to gain a sound understanding of your cyber exposure is to undertake a cyber risk mapping exercise, which involves mapping a company's existing insurance policies against the company's unique cyber exposures and scenarios. It helps organisations better understand their cyber risk profile and empowers them to make informed insurance decisions," says Butler.

A cyber risk mapping excercise can help an organisation better understand their cyber risk profile and empowers them to make informed insurance decisions.

THE LATEST IN CYBER INSURANCE DEVELOPMENT

Marsh has been working closely with insurers to develop cyber insurance solutions in response to the evolving cyber risk landscape. Many of these solutions are aimed at bridging gaps between traditional insurance policies and newer cyber products. Some of the policies that have been developed include:

- **CYBER ECHO** – Aims to provide top-up cover to an existing primary cyber policy. This policy offers the option of a full limit reinstatement, which is typically unavailable under a primary cyber policy.
- **CYBER GAP** – Aims to cover the "cyber gap" created by certain exclusions under a commercial property policy where bodily injury, property damage and business interruption arising from a hacking event are excluded.
- **CYBER CAT** – Aims to cover catastrophic losses typically larger than the self-insured retention levels set by companies.

6 www.insurancebusinessonline.com.au/au/news/breaking-news/lloyds-ceo-cyber-insurance-to-become-a-must-buy-226120.aspx

WHAT'S THE LATEST IN MANDATORY DATA BREACH NOTIFICATIONS?

Amplifying the discussion on cyber risks and cyber insurance is the imminent introduction of mandatory reporting.

With the *Privacy Amendment (Notifiable Data Breaches) Bill 2016* having now passed through both Houses of Parliament, businesses will soon be required to notify the Australian Information Commissioner, as well as all affected parties, in the event of a data breach that meets the applicable harm threshold.

Based on the experiences of countries where similar laws already exist (such as the United States), Australian businesses can expect to face significant financial burden in complying with their notification obligations. In the event of a breach, a company can incur legal costs to determine who must be notified in Australia and overseas, costs to compile notification details of compromised individuals, costs to make the notifications, to set up call centres, to engage public relations consultants and to provide credit monitoring services to affected customers. Fortunately, all of these costs are typically covered by cyber insurance policies, which were designed with such scenarios in mind.

"We expect that increased public awareness of data breaches from mandatory reporting could lead to a fertile class action landscape. Affected parties, alleging misleading deceptive conduct, might then move to recover costs incurred as a result of a breach," warns Butler.

Australian businesses currently face a significant risk of cyber events. This risk will continue to rise in sync with the increasingly digitised world. It is critical for organisations to proactively identify, analyse and manage cyber risk – this includes regularly reviewing the various risk transfer options available, with a serious consideration for cyber insurance solutions.

This article was updated on 13 February 2017 following the Bill's passage through the Senate.

Australian businesses can expect to face significant financial burden in complying with their notification obligations.