ADVERTORIAL

wotton kearney

Government's spotlight on cyber

As the scale, sophistication and frequency of cyber-attacks continue to rise in Australia, Wotton + Kearney considers the impact on the insurance industry of the government's efforts to improve Australia's cyber-resilience and crack-down on e-crime and state-sponsored cyber-attacks.

Kieran Doyle
Partner & Cyber Specialist

> The Australian Government has pledged $1.67 billion to enhance cyber-security capabilities.

Threat landscape

Our growing dependence on technology and our hurried transition to remote working has increased opportunities for malicious cyber-actors to target vulnerable organisations. Crowdstrike reports that there has been a 330 percent increase in cyber-attacks across the Asia Pacific region this year[1]. Since March, the Australian Cyber Security Centre (ACSC) has received an average of two COVID-19 related cyber-crime reports daily[2].

While it has been estimated that cyber-crime costs the Australian economy up to $29 billion per year[3], the potential impact of state-sponsored cyber-attacks against critical infrastructure is even more concerning. The government has projected that a large-scale disruption to critical digital infrastructure could cost the economy $30 billion within a month[4], which is worrying given the concurrent 'economic hibernation' caused by COVID-19[5].

Cyber-crime and cyber-resilience

The ACSC reports that many of the cyber-crime incidents reported over the past year could have been prevented or substantially mitigated[6]. Against that context, it is unsurprising that cyber-resilience is a priority in Australia's recently released 2020 Cyber Security Strategy (Strategy). The Strategy includes $1.67 billion pledged over the next decade to enhance cyber-security capabilities across government, businesses and the community through programs and regulatory reforms. These are aimed at:

- protecting Australia's critical infrastructure and systems of national significance, and
- building cyber security support and standards for businesses, with tailored support for SMEs.

State-sponsored cyber-attacks

On 19 June 2020, Prime Minister Scott Morrison announced that Australian organisations and critical infrastructure were being targeted by a state-based cyber-actor in large-scale 'copy-paste' hacking incidences[7]. While the government did not attribute these attacks to any particular state, it has ramped up its cyber-defence, disruption and resilience capabilities.

On 30 June 2020, the Prime Minister committed $1.35 billion over the decade to enhance the capabilities of the Australian Signals Directorate (ASD) and the ACSC[8]. This investment represents the bulk of the funding proposed under the Strategy and reflects the government's acknowledgement that state-sponsored cyber-attacks have been increasing in frequency[9].

While it is easy for Australian businesses to understand that e-crime actors attack them for financial gain, many don't understand – or are less concerned by – the interest of state-based actors as the focus of the attack is not often disruption, customer data or personal information. While the immediate impact might not be visible, businesses should be very concerned. There are businesses with IP of immediate value to state-based actors, as illustrated by the widely-reported COVID-19 research attacks. Other businesses that have data stolen often don't see the true value of that data until copycat products go on sale and competition drives prices down. For this reason, the government is stepping-in to help protect Australian businesses.

Another big, unanswered question is whether you can prove that an attack was state-sponsored – and if you can, what does this mean? The insurance industry faces its own unique challenges in this regard. In the US case Mondēlez v Zurich[10], an Illinois state court is currently considering whether losses incurred by Mondēlez due to the 2017 Not-Petya cyber-attacks, which have been attributed to Russia[11] and tied to its conflict with the Ukraine, fall within an 'act of war' exclusion in the policy.

While this case is being litigated on a property policy, 'act of war' clauses (also common in cyber policies) are becoming increasingly relevant as advances in forensic technology and intelligence better enables attribution. The insurance industry is closely monitoring this case, as the outcome may have significant consequences on whether attribution is possible, the steps required to achieve it, and whether a cyber-attack can be considered an 'act of war'.

Even putting the attribution question aside, the Australian Government's focus on building public and private sector cyber-capabilities, and increasing cyber-security awareness, can only be a good thing. This should ultimately benefit the insurance industry by reducing the risk profile of preventable cyber incidents.

For more legal and claims insights, visit:
www.wottonkearney.com.au/knowledge-hub

1 https://itbrief.com.au/story/crowdstrike-uncovers-key-cybersecurity-findings-following-covid-19
2 https://www.cyber.gov.au/acsc/view-all-content/advisories/threat-update-covid-19-malicious-cyber-activity-20-april-2020
3 Microsoft and Frost & Sullivan (2018), Understanding the Cybersecurity Threat Landscape in Asia Pacific: Securing the Modern Enterprise in a Digital World
4 https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf; https://www.austcyber.com/resource/digitaltrustreport2020
5 https://www.austcyber.com/resource/digitaltrustreport2020
6 https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf
7 https://www.pm.gov.au/media/statement-malicious-cyber-activity-against-australian-networks
8 https://www.pm.gov.au/media/nations-largest-ever-investment-cyber-security
9 https://www.pm.gov.au/media/statement-malicious-cyber-activity-against-australian-networks
10 Mondelez Intl. Inc. v. Zurich Am. Ins. Co., No. 2018-L-11008, 2018 WL 4941760 (Ill. Cir. Ct., Cook Cty., complaint filed October 10, 2018); https://www.ft.com/content/8db7251c-1411-11e9-a581-4ff78404524e
11 https://www.dfat.gov.au/sites/default/files/australia-attributes-notpetya-malware-to-russia.pdf