Recent actions tackling expanding ransomware threat

wotton kearney

A founding member of LEGALIGN GLOBAL

3 AUGUST 2021

AT A GLANCE:

- Ransomware has established itself as one of Australia's fastest growing cybercrime threats.[1]
- Both the Australian Government and the Opposition have taken recent action against this serious threat, with further changes flagged.
- In June, the Shadow Assistant Minister for Cyber Security introduced a private member's bill, proposing a mandatory ransomware notification regime.
- In July, the Minister for Home Affairs announced the creation of a multi-agency ransomware taskforce – Operation Orcus.
- The issue of ransomware was also addressed in a House of Representatives Committee hearing in late July that heard from IAG, QBE and Marsh. Following the hearing, media reports suggested there is a growing push to ban insurers covering ransom payments.
- For cyber insurers facing heightened risks in a challenging market, this action against the threat of ransomware is welcome news but it could have a significant impact on small business owners that are victims of ransomware attacks.

RANSOMWARE

Ransomware is an intensifying threat to businesses of all sizes.

The Australian Cyber Security Centre (ASAC) has reported a 60% year-on-year increase.[2] According to a recent Cyber Security Industry Advisory Committee report: "In the three months of April to June 2020 alone, there was a 65 per cent increase in cyber security incidents, at an estimated $7.6 billion cost to business for the financial year."[3]

Ransomware is a significant national problem that's also being experienced worldwide, as highlighted by a recent Cyber Security Cooperative Research Centre report that estimated that cybercrime has cost the global economy USD1 trillion.[4]

Beyond the price of the ransom, these attacks cause significant disruption to the targets' operations and significant remediation costs. While some attacks are high profile, such as those recently affecting JBS Foods and Nine Entertainment, many more are quietly crippling SME businesses.

In Australia, both the Government and the Opposition are responding to this significant issue.

OPERATION ORCUS – GOVERNMENT RESPONSE TO RANSOMWARE

Last year, the Government announced its Cyber Security Strategy 2020, which involves investing $1.67 billion over 10 years to create "a more secure online world for Australians, their businesses and the essential services upon which we all depend".[5]

The Cyber Security Strategy 2020 expanded the Australian Federal Police's (AFP) operational capabilities in this area with $89.9 million of funding. The AFP is now leading the recently announced Operation Orcus, a joint operation of the Australian Cyber Security Centre (ACSC), the AFP, the Australian Criminal Intelligence Commission, Austrac and state and territory police forces. Operation Orcus will collect intelligence that "is expected to be used by the ACSC to disrupt ransomware operations run by offshore criminals using offensive cyber operations".[6] According to industry commentary, the Operation Orcus taskforce will:

- "better identify opportunities to disrupt ransomware operations
- strengthen the investigation of ransomware across Australia, and internationally, and
- improve intelligence sharing and coordination between agencies on ransomware and the organised crime groups engaged in ransomware attacks".

On 15 July, the Industry Advisory Committee released its first annual report Cyber Security Industry Advisory Committee Annual Report 2021, which detailed progress on the implementation of the Cyber Security Strategy 2020. This included publishing its first thought leadership piece in March 2021: Locked Out: Tackling Australia's ransomware threat.

On 23 July, the issue of ransomware was also addressed in a House of Representatives Committee hearing that heard from IAG, QBE and Marsh. Following the hearing, a Government MP, Tim Wilson, observed: "It seems pretty clear to me that allowing insurance to reimburse for ransoms just incentivises criminal behaviours, while also increasing premiums for other cyber risks and should be outlawed."[8]

When announcing Operation Orcus, Minister Andrews also urged victims of ransomware attacks to contact the police and the ACSC, and not to pay cyber criminals. The Australian Cyber Security Centre (ACSC) similarly takes the view that companies should not pay ransoms as that can encourage attacks and there is no guarantee that the data will be recovered. There are also concerns those payments may contravene proceeds of crime offences or anti-money laundering laws.

Currently, there is no express prohibition on payments of ransoms for organisations or their insurers. That being said, the question of whether target companies should pay a ransom can be complex.

Often, paying a ransom is the most effective way to minimise business interruption. It can also lower the likelihood that confidential information will be publicly disclosed, including the personal information of individuals who have interacted with the targeted company. However, as the Cyber Security Industry Advisory Committee points out:[9] "Victims are most likely to pay a ransom when they perceive it to be the best option for recovery. However, cybercriminals share information and when they are successful at extracting ransomware payments from victims not only does it re-incentivise them, but also attracts and motivates others, increasing Australia's attractiveness as a target."

While Tim Wilson's position has not formerly been tabled as Coalition policy, further review of the legal treatment of cyber ransoms, including insurance coverage, seems likely.

OPPOSITION ACTION

On 21 June 2021, Shadow Assistant Minister for Cyber Security, Tim Watts, introduced the *Ransomware Payments Bill 2021,* a private member's bill that proposes a mandatory ransomware notification regime. If passed, this will require notification, as soon as practicable, to the ACSC when an entity makes ransomware payments to end an attack, for example to avoid encrypted data being decrypted or prevent data being published, damaged or destroyed.

The Bill proposes notification needs to include:

- information about the attacker such as their identity (if known)
- a description of the ransomware attack
- details of the cryptocurrency wallet to which payment is made
- amount of the ransom demanded, and
- any indicators of compromise.

The Bill is designed to allow ACSC to better gather and distribute real time threat intelligence to improve the efficacy of the law enforcement response, and Australia's ability to cooperate with international efforts tackling ransomware. It is also designed to promote broader awareness of the ransomware threat and mitigation options to improve Australia's cybersecurity preparedness.

THE ISSUES FOR INSURERS AND THEIR CUSTOMERS

The establishment of Operation Orcus is positive news for cyber insurers, who are facing heightened risks in a challenging market. Any improvement, forced or otherwise, in a business' ability to repel attacks should drive down losses for insurers and their insureds, which would be most welcome given the market is already under pressure despite still being quite immature compared to other markets.

Cyber insurance policies usually include coverage for payment of ransoms. It appears that there is a growing push to ban insurers covering ransom payments, however it remains unclear whether this will deter ransomware actors. While it is a last resort, some businesses often have little choice but to pay because the cost of not doing so – business failure – is too great. This is particularly a vexing issue for small businesses who simply don't have the resources to better protect themselves in the first place. The multi-jurisdictional nature of ransomware attacks is also likely to be a factor, as Australian action without international coordination may prove ineffective.

> **Both the Australian Government and Opposition have taken recent action against this serious threat, with further changes flagged.**

If insurance coverage of ransoms is prohibited, it is unlikely that the problem will simply go away. This is predicted by the 90s experience with kidnapping. When ransom payments were banned in the 90s for kidnap insurance, it didn't stop the kidnapping. Rather it put more pressure on families and businesses to pay out of their own pockets.

According to one author: “Outlawing ransom payments, which several countries attempted to do, did not result in discernible declines in kidnappings.”[10] Others commented: “…Countries that do not make concessions [ie. ransom payments] experience far worse outcomes for their kidnapped citizens than countries that do. …There is no evidence that American and British citizens are more protected than other Westerners by the refusal of their governments to make concessions.” While ransomware is not a direct life or death situation like kidnapping can be, an attack could well be a death sentence for an SME business.

For insurers, a government ban on ransom payment coverage will make some decisions simple. But, arguably, such a position could increase losses under a cyber policy due to extended business interruption and increased costs. While this statement should not be read as advocating ransom payments, an approach involving preventative measures and better equipping businesses to respond to incidents, particularly small businesses, may prove less costly for all concerned.

REFERENCES:

[1] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020-annual-report-2021.pdf
[2] https://www.abc.net.au/news/science/2021-07-16/australian-organisations-paying-millions-ransomware-hackers/100291542
[3] https://www.homeaffairs.gov.au/cyber-security-subsite/files/tackling-ransomware-threat.pdf
[4] https://www.abc.net.au/news/science/2021-07-16/australian-organisations-paying-millions-ransomware-hackers/100291542
[5] https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/australia%E2%80%99s-cyber-security-strategy-2020
[6] https://www.itnews.com.au/news/afp-leading-new-cross-agency-ransomware-taskforce-567623
[7] https://www.cybersecurityconnect.com.au/strategy/6970-afp-to-lead-new-operation-against-ransomware
[8] https://www.afr.com/companies/financial-services/insurers-call-for-death-of-cyber-ransom-payments-20210628-p584vf
[9] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020-annual-report-2021.pdf
[10] Jenkins, 2018, p20
[11] Mellon, Bergen and Sterman, 2017, p13

wotton kearney

Need to know more?

For more information please contact our authors.

Kieran Doyle
Partner & Cyber Team Leader
T: +61 2 8273 9828
Email Kieran

Samuel Hartridge
Senior Associate
T: +61 2 9064 1872
Email Samuel

Ronny Raychaudhuri
Associate
T: +61 2 9064 1833
Email Ronny

Our specialist cyber services & team

W+K has a dedicated 16-strong team of cyber specialists across Australia and New Zealand, ready to assist with all your incident response, regulatory, policy coverage and claims needs.

DOWNLOAD OUR CONTACT CARD

MORE W+K CYBER INSIGHTS

OUR GLOBAL CYBER SERVICES