HERBERT SMITH FREEHILLS

CYBER-RANSOMS ARE ON THE RISE: WHAT DO YOU NEED TO KNOW?

18 November 2021
Legal Briefings – By **Tania Gray, Christine Wong and Hilary Starr**

‘Cyber-ransoms’ are on the rise, and with new cyber tactics and ways of working, the risks are increasing.

KEY TAKEAWAYS

- A key question facing companies is whether or not to pay a cyber-ransom following a cyber-attack.
- This is not a straightforward decision – there are a number of legal and practical issues at play.
- At the same time, the payment of ransoms is facing increased scrutiny from governments and insurers across the world.
- As governments focus on cyber security and explore new policies to deter attacks, companies will need to be ready to adapt. So, what should you be thinking about?

WHY IS THIS IMPORTANT?

Cyber ransoms are on the rise, and the risks to businesses are increasing

Globally, it is estimated that there is a ransomware attack on a business every 11 seconds.[1]

The number of reported cyber-attacks has surged since COVID-19, with factors such as remote working likely contributing to the increase.[2]

As companies transition to new ways of working for the longer term and increased sophistication of threat actors, these risks are likely to stick around.

The Australian Government's recent *Ransomware Action Plan*[3] stressed the growing threat posed by ransom attacks, providing insight into the tactics used by cyber-criminals:

- Sophisticated attackers are likely to employ a targeted approach, which may involve trawling through stolen data, and demanding a ransom payment that is equivalent to the insured amount in a company's policy.[4]
- A recent report from Allianz noted that less sophisticated attackers are likely to employ a "scattergun" approach. With ransomware available for as little as $40 for a monthly subscription, there is a very low "knowledge threshold" to carry out these attacks.[5]
- An emerging trend of "double" and even "triple" extortion has also been highlighted. Under this approach, cyber criminals will demand further payments (i.e. after an initial ransom has been paid) to return data stolen in an attack, threatening to leak information if this is not provided.[6]

The impact of ransom attacks can be devastating.

By the end of 2021, damages associated with ransomware are projected to reach US$20 billion globally.[7]

With increasing risks, new tactics, and significant possible loss, companies cannot afford to ignore this issue.

SO, SHOULD I PAY A CYBER-RANSOM?

This isn’t a straightforward decision – there are commercial considerations at play but depending on the circumstances and identity of the attacker, it may be illegal to pay

Given the frequency of attacks, and the significant damage that can arise, it is important to have a plan in place if your company is the victim of a cyber ransom attack.

A key question is whether to pay the ransom.

The answer is not straightforward. Commercial and practical issues such as the likelihood of recovering data, a company's insurance coverage, the potential costs of remediation, and reputational and regulatory issues will all be relevant. There is also a fundamental question which cannot be overlooked - **it is legal to pay a cyber-ransom?**

The answer is not clear cut. There is no specific blanket offence prohibiting payment of all cyber-ransoms. However, a number of offences could be triggered by the payment of a ransom in response to a cyber-attack.

Potential areas of liability include:

- **Sanctions:** Australia's sanctions laws apply where a payment is made to a banned person or entity, or into a particular sanctioned jurisdiction. Liability here is broad - the payment can be direct, or indirect, and companies can be liable even where there is no knowledge that the payment is being made to a sanctioned entity. There have been recent proposals to expand the scope of Australia's sanctions laws, including to target cyber activity[8] watch this space. These types of specific sanctions already apply in other jurisdictions like the US.

- **Proceeds of crime:** Payment of a ransom could also raise issues under laws relating to the proceeds and instruments of crime. There is a possibility that funds used to pay the ransom could be used in the commission of further offences by the cyber-attacker, making the payment an "instrument of crime." This will depend on the circumstances of the case.

- **Terrorism financing:** There may also be issues under terrorism financing laws. This will come down to the identity of the cyber-criminal, and their motivations. Increasing geopolitical tensions could drive up activity and risks in this area.

It might seem an unfair result that a company, as the victim of a cyber-crime, might be committing an offence by paying a ransom. In this scenario, there are also range of defences that might apply. These will depend on the circumstances of the attack, including whether a company has acted reasonably in response to a threat or emergency. For defences to sanctions offences, the systems and processes the company had in place to manage risks before the attack are also relevant.

One of the key factors that may trigger liability, but also the availability of any defences, will be the identity of the cybercriminal.

Companies should consider what steps they can take to identify the cyber-criminal, or at the very least, the malware used. This will also have practical implications for remediation.

WHAT ABOUT INSURANCE?

The market for cyber-specific insurance in Australia is developing but is still relatively immature.[9]

With coverage unclear in a changing landscape, insurance is not a cyber-security 'silver bullet'

Currently, a number of Australian insurers offer policies which expressly cover the payment of a ransom in response to cyber-attacks.[10] However, even where a policy covers cyber-ransoms, a number of important exclusions may apply.[11]

Companies may also find themselves covered by non-affirmative or "silent" cyber, which describes cyber risks that are neither expressly covered or excluded from more general insurance policies, such as business interruption.[12]

This means that coverage in the event of a ransom attack is often uncertain.

While it remains a legal grey area, the practice of paying ransoms by insurers has come under increasing scrutiny.

In its *Ransomware Action Plan*, the Government stressed its 'zero tolerance' approach to the payment of ransoms.

This was echoed in a recent report from an industry research body, the Cybersecurity Cooperative Research Centre (**CSCRC**), which criticised the payment of ransoms by insurers, claiming it "fuelled" the ransomware trade, and put "extraordinary pressure" on the insurance industry.[13] The CSCRC ultimately recommended that the paying of ransoms by insurers be prohibited.

This issue has recently received government attention,[14] and is clearly a developing issue.

For companies considering their insurance needs, it is important to note that cyber insurance is not a 'silver bullet' and cannot replace a holistic cyber-security strategy.

You can read more about the global landscape for cyber-insurance here.[15]

WHAT ELSE DO I NEED TO KNOW?

A company facing a ransom will have to grapple with a range of issues, including reputational, operational and legal.

Start preparing now

This may include reporting obligations – including the introduction of mandatory reporting to the Australian Cyber Security Centre[16]

Companies should plan ahead to avoid making these critical decisions in the heat of a crisis.

To minimise the risks of cyber-ransom attacks, and consider options ahead of time, companies should consider:

- Following 'cyber hygiene' best practice – this is the first line of defence. Take a look at the ACSC's guidelines;[17]
- Developing an Incident Response Plan to manage key stakeholders (including reporting obligations and communications with affected persons), and engaging cyber-security specialists;
- Proactively engage with legal advisors, including to manage flow-on legal risks such as class actions and regulators; and
- Considering the company's stance in relation to the payment of cyber ransoms in the event of an attack.

WHAT NEXT?

Stay tuned for our next article in this series which will be looking at regulatory enforcement action following a data breach.

View our Cyber in Australia insights

---

1. Australian Government,*Ransomware Action Plan* (13 October 2021), https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf, 2.

2. Australian Cyber Security Centre (**ACSC**) *Annual Cyber Threat Report 2020-21*, https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21. Marsh McLennan, *MMC Cyber Handbook 2021*, https://www.marshmclennan.com/insights/publications/2020/october/mmc-cyber-handbook-2021-.html.

3. Australian Government (n 1).

4. Australian Government (n 1) 2-4.

5. Allianz Global Corporate and Specialty, *Ransomware Trends: Risks and Resilience* (October 2021), https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/agcs-ransomware-trends-risks-and-resilience.pdf, 3.

6. Allianz Global Corporate and Speciality (n 5) 4.

7. Australian Government (n 1) 2.

8. Herbert Smith Freehills, *Proposed Reforms to Australia's Sanctions Regime to Target Corruption, Cyber-Crime, Human Rights Violations*, https://www.herbertsmithfreehills.com/latest-thinking/proposed-reforms-to-australia%E2%80%99s-sanctions-regime-to-target-corruption-cyber-crime.

9. CSCRC, *Underwritten or Oversold Report* (October 2020),https://cybersecuritycrc.org.au/sites/default/files/2021-10/Underwritten%20or%20oversold%20%20-%20DV.pdf, 6.

10. OECD,*Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation* www.oecd.org/finance/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf.

11. See, for example, litigation related to insurance for the 2017 Notpetya attacks: OECD*Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation* (2020), www.oecd.org/finance/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf, 10-11.

12. Marsh McLennan (n 2).

13. CSCRC (n 9) 13.

14. See statements made by Nick Hawkins (CEO of IAG) to the House of Representatives

Standing Committee on Economics (25 June 2021), https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22committees%2Fcommrep%2F8472be85-cc92-461d-83c6-5c0d844e5a5b%2F0000%22, 50.

15. Herbert Smith Freehills, *Are You Cyber Insurance Fit?*, https://www.herbertsmithfreehills.com/latest-thinking/are-you-cyber-insurance-fit.

16. Herbert Smith Freehills, *Mandatory Notification of Ransomware Payments on Australia Appears Likely* (22 June 2021), https://www.herbertsmithfreehills.com/latest-thinking/mandatory-notification-of-ransomware-payments-in-australia-appears-likely.

17. ACSC, *Essential Eight*, https://www.cyber.gov.au/acsc/view-all-content/essential-eight.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

TANIA GRAY
PARTNER, SYDNEY

+61 2 9322 4733
Tania.Gray@hsf.com

CHRISTINE WONG
PARTNER, SYDNEY

+61 2 9225 5475
Christine.Wong@hsf.com

PETER JONES
PARTNER, SYDNEY

+61 2 9225 5588
peter.jones@hsf.com

LEGAL NOTICE