Should it be the end of the line for ransom cover?

14 OCTOBER 2021

wotton kearney

A founding member of LEGALIGN GLOBAL

AT A GLANCE:

- On 13 October 2021, the Australian Government released its **Ransomware Action Plan** that proposes, among other things, for certain companies to have mandatory reporting obligations for ransomware attacks.
- A Cyber Security Cooperative Research Centre policy paper on cyber insurance suggests cover for ransom payments should be banned.
- Is insurance really the problem? Ransomware cover is a balancing act, but insurers are just one piece of a complex puzzle.

Tackling ransomware attacks is top of mind for the Australian Government, which released its Ransomware Action Plan on 13 October[1]. The plan includes the introduction of mandatory ransomware attack reporting requirements for companies with a turnover of over $10 million – with potential civil penalties if they do not comply.

At the same time, insurers are coming under scrutiny – including in a policy paper published on 12 October 2021 by the Cyber Security Cooperative Research Centre – for potentially playing a part in increasing ransomware attacks by extending cover for ransom payments.

There is no question that ransomware is an ever-growing threat. According to the Australian Cybersecurity Centre, there has been a 60 per cent increase in ransomware attacks against Australian entities in the past year[2]. However, addressing the threat is not straight-forward.

It's worth challenging whether excluding cover for ransom payments really is the answer to this complex issue. Perhaps the focus should be on the source of the attacks themselves, as presented by the Ransomware Action Plan, while also working to identify and prosecute threat actors and incentivising companies to bolster their cyber security. This approach is likely to have better outcomes than restricting the support available for companies that suffer an attack.

> The Ransomware Action Plan sets the stage for the steps the Australian government plans to take to address the ransomware threat. Some key reforms in the pipeline include introducing:
>
> - mandatory ransomware attack reporting requirements
> - a stand-alone offence for cyber extortion
> - a stand-alone aggravated offence for cybercriminals targeting critical infrastructure, and
> - amendments to ensure law enforcement can seize or freeze the proceeds of cybercrime.

HOW OFTEN ARE RANSOMS BEING PAID?

CrowdStrike's *Global Attitude Survey 2020* surveyed 200 senior IT professionals in Australia. It found that two thirds of the companies surveyed had suffered a ransomware attack between November 2019 and November 2020 and, of those, only one third had paid the ransom[3].

A recent survey by the International Data Corporation found that 60% of companies who responded "probably would" pay a ransom if an attack significantly hampered their operations. Of these, around a third would only do so if they had insurance in place – the remainder would do so regardless of whether or not they had insurance[4].

Ransomware events can affect businesses in a variety of ways, which range in intensity and the extent to which they can be managed or remediated. The impacts can be long and devastating or they can be fairly short-lived. The rapid increase in double extortion, where threat actors threaten misuse of exfiltrated company data in addition to encryption, has upped the ante significantly for entities facing ransomware attacks.

Once entity data is out in the open, there are even more risks to consider – including risks facing individuals whose personal information has been taken.

Coveware's 2021 Q2 report noted that 81% of ransomware attacks in the quarter involved a threat to leak exfiltrated data – however despite this significant statistic, the number of companies that actually paid a ransom in response decreased from 65% in the previous quarter to 50%[5].

It is difficult to trace whether the availability of insurance cover has actually led to more ransomware attacks or more ransoms being paid. Even if ransomware attacks become more common, it does not necessarily follow that the rate of ransom payments is following the same trajectory. Clearly insurance is not the only factor in play.

SO ARE INSURERS "HELPING DRIVE THE ILLICIT RANSOMWARE TRADE"?

The question of whether the existence of insurance promotes, or somehow tacitly supports, crime has been asked for decades regarding kidnapping, ransom and extortion (KRE) insurance. While there's little evidence to support the claim, there are examples of how a lack of insurance can hinder government's efforts to tackle the crime. For example, in 1991 Italy banned KRE insurance and ransom payments. This had the unfortunate result that some families simply didn't report kidnappings to authorities at all.

This example highlights how insurance can help assist those in trouble, as well as provide data to help authorities tackle the crime at its source. The importance of tackling the crime at its source is highlighted in the Government's Ransomware Action Plan and reflected in its plans for mandatory reporting of ransomware incidents, and perhaps in time also ransom payments.

With ransomware attacks, companies face very difficult decisions that have to be made under pressure and with urgency. The range of relevant considerations depends on the company's industry, the information they have and how they were targeted.

Certainly, another consideration is the availability of insurance cover for ransom reimbursement. However, it does not follow that the existence of an insurance policy itself will cause an insured to pay a ransom. In our experience many businesses, particularly SMEs, are simply focused on making decisions that will keep them afloat – regardless of who is picking up the bill.

HOW CAN THE INSURANCE MARKET RESPOND?

Ransom payment cover, while crucial for many businesses, is designed to be a last resort. In this regard, the role of insurers is to be sensitive to an insured's needs in a crisis. For example, Marsh's ransomware incident response guide lists paying the ransom as just one tool in an insured's toolbox[6]. The availability of cover does not mean the decision to consider paying a ransom is not fraught or that the cover is without conditions. Insurers can have stringent measures in place to ensure AML-CTF obligations are complied with. They can also place other conditions on cover to ensure it is only accessed in the appropriate circumstances.

The cyber insurance market and underwriting standards are hardening because of the increased risks, and yet the demand for cyber insurance will continue to increase in line with the risks.

As the renewal cycle continues over the next year or so, insureds will likely be forced to tighten their cybersecurity, making ransomware attacks more difficult to pull off. Contrary to popular belief, ransomware threat actors are not necessarily always sophisticated hackers. The issue is often that companies are poorly prepared and don't recognise the gaps in their cybersecurity.

Raising the barrier for attack will reduce the risk of an attack being successful and make it less profitable for malicious actors. In line with the Ransomware Action Plan, this suggests a focus on incident preparedness will be key.

The path is open to insurers to exclude ransom payments cover from cyber insurance policies. However, such terms are unlikely to be very attractive to brokers and insureds in the current climate and is unlikely to have the desired effect of curbing the rise in ransomware attacks. Instead, future reform can be focused on two priorities – identifying and prosecuting cybercriminals, and incentivising businesses to be better prepared for ransomware and other cyber incidents.

If you need support in recovering from a ransomware attack, please get in touch and we can use our extensive claims experience on the ground with insureds facing cyber events to guide your decision-making.

REFERENCES:

[1] https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf

[2] https://www.abc.net.au/news/science/2021-07-16/australian-organisations-paying-millions-ransomware-hackers/100291542

[3] https://www.crowdstrike.com/resources/reports/global-attitude-survey-2020/

[4] https://www.idc.com/getdoc.jsp?containerId=prAP48115421

[5] https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority

[6] https://www.marsh.com/th/en/migrated-articles/40-million-ransom-do-you-pay.html

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

Jessica Chapman
Associate

T: +61 2 8273 9876
Email Jessica

Get in touch with our cyber specialists

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