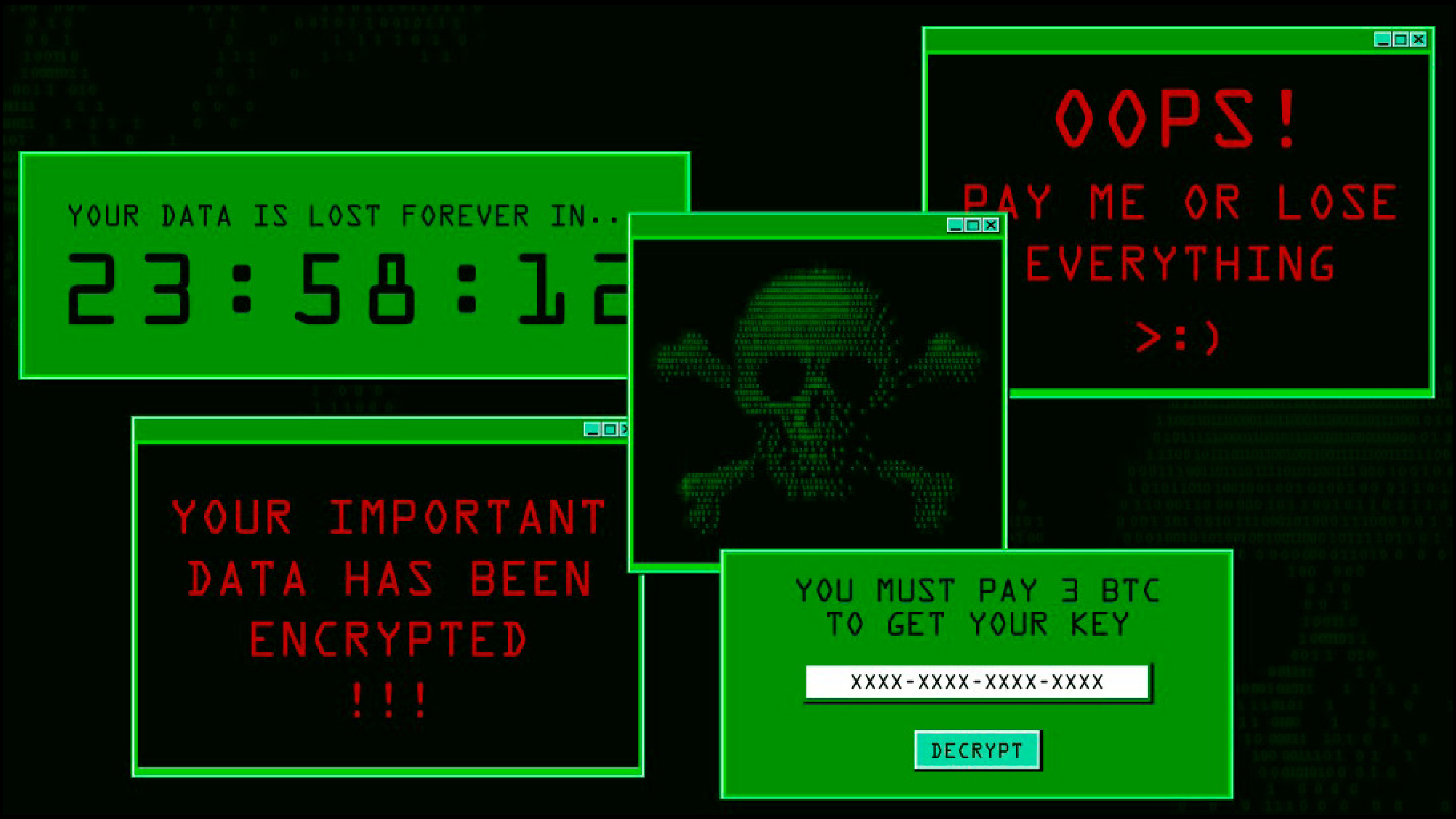
Exfiltrate, encrypt, extort

The global rise of ransomware and Australia's policy options

Rachael Falk and Anne-Louise Brown


YOUR DATA IS LOST FOREVER IN..
23:58:12
OOPS!
PAY ME OR LOSE EVERYTHING
>:)
YOUR IMPORTANT DATA HAS BEEN ENCRYPTED !!!
YOU MUST PAY 3 BTC TO GET YOUR KEY
XXXX-XXXX-XXXX-XXXX
DECRYPT

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
INTERNATIONAL CYBER POLICY CENTRE
TWENTY YEARS OF ASPI STRATEGY 2001 - 2021

Policy Brief
Report No. 47/2021

About the authors

Rachael Falk is the Chief Executive Officer of the Cyber Security Cooperative Research Centre.

Anne-Louise Brown is the Director of Corporate Affairs, Cyber Security Cooperative Research Centre.

Acknowledgements

Thank you to Danielle Cave for all of her work on this project. Thank you also to all of those who peer reviewed this work and provided valuable feedback including Michael Sentonas, Dr Natasha Molt, Fergus Hanson, Michael Shoebridge, Bart Hoogeveen, Jocelinn Kang and Tom Uren. ASPI's International Cyber Policy Centre receives funding from a variety of sources including sponsorship, research and project support from across governments, industry and civil society. The Cyber Security CRC is a bronze sponsor of the centre. No specific funding was received, from any organisation, to fund the production of this report.

What is ASPI?

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our annual report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements.

ASPI International Cyber Policy Centre

ASPI's International Cyber Policy Centre (ICPC) is a leading voice in global debates on cyber, emerging and critical technologies, issues related to information and foreign interference and focuses on the impact these issues have on broader strategic policy. The centre has a growing mixture of expertise and skills with teams of researchers who concentrate on policy, technical analysis, information operations and disinformation, critical and emerging technologies, cyber capacity building, satellite analysis, surveillance and China-related issues.

The ICPC informs public debate in the Indo-Pacific region and supports public policy development by producing original, empirical, data-driven research. The ICPC enriches regional debates by collaborating with research institutes from around the world and by bringing leading global experts to Australia, including through fellowships. To develop capability in Australia and across the Indo-Pacific region, the ICPC has a capacity building team that conducts workshops, training programs and large-scale exercises for the public and private sectors.

We would like to thank all of those who support and contribute to the ICPC with their time, intellect and passion for the topics we work on. If you would like to support the work of the centre please contact: icpc@aspi.org.au

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional.

ASPI

Tel +61 2 6270 5100
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_ICPC

First published July 2021.

ISSN 2209-9689 (online), ISSN 2209-9670 (print).

Cover image: Produced by Jake Moody of Leading Hand Design

No specific sponsorship was received to fund production of this report.

Exfiltrate, encrypt, extort

The global rise of ransomware and Australia's policy options

Rachael Falk and Anne-Louise Brown

Policy Brief
Report No. 47/2021

Contents

What's the problem?

As the Covid-19 pandemic has swept across the world, another less visible epidemic has occurred concurrently—a tsunami of cybercrime producing global losses totalling more than US$1 trillion.[1] While cybercrime is huge in scale and diverse in form, there's one type that presents a unique threat to businesses and governments the world over: ransomware.

Some of the most spectacular ransomware attacks have occurred offshore, but Australia hasn't been immune. Over the past 18 months, major logistics company Toll Holdings Ltd has been hit twice; Nine Entertainment was brought to its knees by an attack that left the company struggling to televise news bulletins and produce newspapers; multiple health and aged-care providers across the country have been hit; and global meat supplies were affected after the Australian and international operations of the world's largest meat producer, JBS Foods, were brought to a standstill. It's likely that other organisations have also been hit but have kept it out of the public spotlight.

A current policy vacuum makes Australia an attractive market for these attacks, and ransomware is a problem that will only get worse unless a concerted and strategic domestic effort to thwart the attacks is developed. Developing a strategy now is essential. Not only are Australian organisations viewed as lucrative targets due to their often low cybersecurity posture, but they're also seen as soft targets. The number of attacks will continue to grow unless urgent action is taken to reduce the incentives to target Australian companies and other entities.

What's the solution?

All governments, civil society groups and businesses—large and small—need to know how to manage and mitigate the risk of ransomware, but organisations can't deal with the attacks on their own. Given the significant—and increasing—threat ransomware presents to Australia, new policy measures are fundamental to dealing with this challenge. While there's no doubt ransomware is difficult to tackle using traditional law enforcement methods because the criminal actors involved are usually located offshore, there are domestic policy levers that can be pulled, for example, to support cybersecurity uplift measures across the economy. Such action is essential because the grim reality is that, when it comes to ransomware, prevention is the best response.

This policy report addresses key areas in Australia where new policies and strategies and improved guidance are needed and also where better support for cybersecurity uplift can be achieved. Our recommendations include arguments for greater clarity about the legality of ransomware payments, increased transparency when attacks do occur, the adoption of a mandatory reporting regime, expanding the official alert system of the Australian Cyber Security Centre (ACSC), focused education programs to improve the public's and the business community's understanding and, finally, incentivising cybersecurity uplift measures through tax, procurement and subsidy measures. We also recommend the establishment of a dedicated cross-departmental ransomware taskforce, which would include state and territory representatives, that would share threat intelligence and develop federal-level policy proposals to tackle ransomware nationally.

Introduction: What's ransomware?

Ransomware is a form of malware designed and deployed by state and non-state cybercriminals who seek out vulnerabilities in the computer systems of organisations, both large and small, locking up, encrypting and extracting data, and rendering computers and their files unusable.[2] Attacks are accompanied by a demand for ransom to be paid in return for decrypting and unlocking systems. Increasingly, ransomware attacks include an extortion element that usually involves threats to leak stolen data publicly or on the dark web if payment isn't made (known as 'hack and leak') to exert pressure on the victim to pay the ransom.

Furthermore, payments can be difficult to trace because they're generally made using cryptocurrency.[3] This also makes it hard—but not impossible (as we saw with the Colonial Pipeline attack)—to investigate and prosecute the criminals responsible for ransomware attacks. Generally, those criminals operate with impunity in extraterritorial jurisdictions (most notably Russian threat actors) where governments protect or tolerate them or don't have the legal systems, frameworks or capabilities in place to prosecute them.[4]

Ransomware is a form of cybercrime that's both scalable and able to be commoditised. It can be bought as a service, generally on the dark web, where ransomware criminals essentially act as 'guns for hire'. In 2020, a US analysis found buying malware online was 'incredibly easy', and that advanced malware tools sell for as little as US$50.[5] The analysis also found that 'almost all premium malware sellers provide buyers with in-depth tutorials and ideas about using their products for technically unskilled buyers.'[6]

The most common way ransomware is deployed into a system is via email phishing campaigns, remote access vulnerabilities and software vulnerabilities.[7] In the case of phishing, a criminal sends an email containing a malicious file or link that deploys malware when it's clicked. Phishing campaigns continue to evolve and are becoming increasingly sophisticated and targeted. Remote access vulnerabilities, such as weak username and password combinations, allow criminals access to and control of the computer remotely. Cybercriminals exploit such vulnerabilities via sustained attacks or by obtaining user credentials, which are often purchased on the dark web, enabling the deployment of malware onto a system.[8] Finally, cybercriminals leverage security weaknesses in popular software programs to gain control of systems and deploy ransomware.[9]

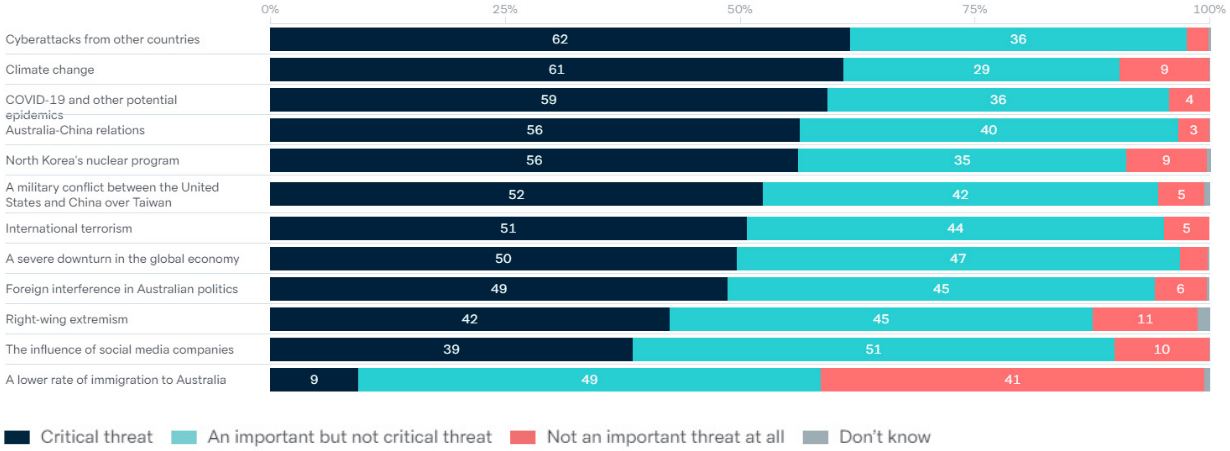
It's important to note that ransomware attacks are entirely foreseeable and almost always defendable. In the physical world, organisations pay for security alarms, high fences and sensors to protect their property. And the digital world should be no different. Ransomware is simply another crime type and the threat should be viewed as another organisational risk because, behind every ransomware attack, are cybercriminals who have watched their victim's network, laying the ground for encryption and data theft to hold the victim to ransom.

The domestic landscape

In 2019–20, the ACSC reported an increase in the number of ransomware attacks on Australian organisations, although specific metrics weren't released.[10] According to the ACSC, the top five sectors to *report* ransomware incidents during that period were health; state and territory governments; education and research; and transport and retail.[11] It's worth noting that the health sector was disproportionately affected, in line with global trends,[12] reflecting its attractiveness as a target due to the value of the troves of personal health data stored and, most importantly, the criticality of the services provided. Put simply, a ransom is more likely to be paid if human life is endangered.

It should be noted that transnational cyberattacks are a serious concern for Australians. The recently published results of the 2021 Lowy Institute Poll reported that 98% of the poll's nationally representative sample viewed 'cyber attacks from other countries' as a critical (62%) or important (36%) threat to Australia over the next decade.[13] That makes transnational cyberattacks the highest of the 12 threats to Australia's vital interests that the Lowy Institute asked people about, rating higher than climate change, Covid-19 and other potential epidemics, international terrorism, a severe downturn in the global economy and Australia–China relations.

Figure 1: Threats to Australia's vital interests



Source: Lowy Institute Poll 2021, online.

Do Australians understand what ransomware is?

In a bid to better gauge the public's understanding of what ransomware is, what it does and what to do in the event of an attack, the Cyber Security Cooperative Research Centre conducted a nationally representative online survey of 1,000 Australian adults in April 2021 on 'Understanding ransomware'. The results—though not unexpected—painted an alarming picture of just how little the Australian public understands ransomware.

Twenty-five per cent of respondents said ransomware was the most significant cybersecurity threat to Australian businesses, coming in behind hacking (48%). Seventy-seven per cent said they wouldn't know what to do if they fell victim to a ransomware attack but, when given a set of options, 56% said they would contact the ACSC. Of the respondents, 42% said they understood how a ransomware attack occurred, and 44% indicated that they knew what happened in a ransomware attack. Respondents believed financial gain was the key aim of an attack (71%), followed by data theft (14%).

While this survey wasn't exhaustive, it clearly shows that the community, generally, has little understanding of ransomware, illustrating that a more concerted effort to educate Australians about it is required. That effort should be teamed with effective tools and policies to mitigate the risk of falling victim to a ransomware attack.

Major reported ransomware attacks in Australia in 2020 and 2021

Major attacks on Australian targets in 2020 and so far in 2021 included the following:

- **February and May 2020: Toll Holdings**

  Employee and commercially sensitive data was stolen in two separate ransomware attacks on Toll Holdings, which is an Australian logistics giant.[14] Some of the stolen data was leaked on the dark web.[15] It's understood that Toll didn't pay either ransom.[16] As a result of the attack, the company has undertaken substantial remediation and cybersecurity uplift programs.[17]

- **May 2020: BlueScope Steel**

  A ransomware attack on a US-based system of BlueScope Steel had global ramifications, affecting production at the organisation's Port Kembla facility in Australia.[18] Details of the attack, including whether payment was made, were undisclosed.

- **June 2020 (two attacks): Lion Dairy and Drinks**

  Dairy processor and drink manufacturer Lion was forced to shut down production as a result of two separate ransomware attacks, which had significant impacts on its vast domestic supply chain.[19] Sensitive data was stolen in the attacks, and the criminals responsible threatened to publish it on the dark web.[20] It's unknown whether a ransom was paid.

- **December 2020: Law in Order**

  Law in Order provides document-management services to the legal profession and purports to have 'iron-clad security'.[21] The criminals who attacked it threatened to publish stolen data on the dark web.[22] It's unknown whether a ransom payment was made.

- **March 2021: Nine Entertainment**

  In late March, Nine Entertainment's news and newspaper production were severely damaged by a ransomware attack.[23] As a result, news teams were forced to work remotely, and most production had to be done out of Nine's Melbourne office, which was the least affected. It took weeks for production to return to normal.[24] It's unknown whether the ransom was paid.

- **March 2021: Eastern Health**

  Eastern Health, which operates several hospitals in Melbourne, was brought to a halt by a ransomware attack that resulted in multiple surgery cancellations and prevented access to patient medical records, internal emails and IT systems.[25] Systems were reportedly damaged for weeks. It's unknown whether a ransom was paid.

- **April 2021: Uniting Care Qld**

  Uniting Care Qld, which operates several hospitals and disability and aged-care facilities across the state, had its access to internal IT systems and patient records severely compromised in a ransomware attack attributed to the REvil group.[26] It's unknown whether a ransom was paid.

- **June 2021: JBS Foods**

  JBS Foods, the world's largest meat supplier, had its global production brought to a standstill by a ransomware attack affecting 47 facilities in Australia.[27] The company confirmed that it paid US$11 million to the attackers.[28]

Ransomware payments and regulating cryptocurrency

Cryptocurrencies are the preferred channel of payment for ransomware attacks because of the assumed untraceability of those payments. However, successful steps are being taken to crack down on cryptocurrency providers via law enforcement and recovery action. In the US, steps have been taken to regulate the use of cryptocurrencies more tightly and to recoup stolen funds; for example, US$2.3 million was recovered after the Colonial Pipeline ransomware attack.[29]

The US Treasury announced in May 2021 that, under a proposed reporting regime, cryptocurrency transfers of more than $10,000 would have to be reported to the Internal Revenue Service—a step that could help to improve the effectiveness of cryptocurrency tracking.[30] There's also a move in the US towards KYC ('know your customer') and AML (anti-money-laundering) cryptocurrency regulation. KYC policies govern the types of information banks must collect, and retain, about their customers; AML regulations require financial institutions to monitor the use of funds by their customers.[31]

In 2018, new laws came into force in Australia making it compulsory for digital currency exchange providers operating in Australia to register with AUSTRAC and comply with reporting obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.[32] Under those laws, exchanges are required to collect information to establish a customer's identity, monitor transaction activity and report transactions or activity that's suspicious or involves amounts of cash over $10,000.[33]

The legality of ransomware payment in Australia

When a ransomware attack occurs, any payment made has legal implications, but in Australia the legality of such a payment is murky at best. This is an issue that needs to be addressed with haste, without the burden of bureaucratic process and a regulatory quagmire. Importantly, criminalising ransomware payment isn't the solution. Mandatory reporting of ransomware attacks, however, should be considered.

The ACSC's advice on payment is clear: don't pay.[34] At first blush, that appears to be straightforward, but any organisation faced with a ransomware attack (in which often every minute matters) grapples with the legal consequences of paying or not paying. This is a highly nuanced issue and one that other nations are also grappling with.

While the payment of a ransom should always be a last resort, criminalisation wouldn't incapacitate the real offenders; nor would it bring restitution to victims. In fact, it would have the effect of further victimising the victim. There are also ethical considerations that need to be taken into account, the central one being the notion that criminalisation could punish organisations for taking proportionate action to protect stakeholders and the community more broadly. This is especially relevant in relation to critical infrastructure entities.

In the Australian context, the Criminal Code Act's 'instrument of crime' provisions are broad. It's an offence to 'deal with' money or other property if there's a risk that the money or property will become an instrument of crime or if the payer is 'reckless' or 'negligent' about the fact that the money or property will become an instrument of crime.[35] The Criminal Code also includes terrorism funding offences, which make it illegal to intentionally 'make funds available to a [terrorist] organisation' if the funder either knows that the organisation is a terrorist organisation or is reckless about whether the organisation is a terrorist organisation.[36]

Australia is also bound by UN sanctions laws and, under the *Charter of the United Nations Act 1945* (which implements UN Security Council sanctions), it's an offence to transfer assets to sanctioned people and entities or to contravene UN sanctions enforcement laws.[37] Currently, no ransomware actors are explicitly listed on the UN's sanctions list; however, sanctions laws could apply in relation to sanctioned states or to groups acting on behalf of sanctioned entities.[38]

The most commonly cited potential defence against a charge of making an 'illegal' ransomware payment is duress. A duress defence can be used if a person 'reasonably believes' that a threat made will be carried out unless an offence of ransom payment is committed, there's no reasonable way the threat can be rendered ineffective, and the conduct or payment is a reasonable response to the threat.[39] Such a defence would depend on the particular circumstances facing an organisation and its payment of a ransom.

In the US, where the Federal Bureau of Investigation (FBI) reported 2,474 ransomware incidents in 2020, ransom payment isn't illegal.[40] However, a ransomware advisory published by the US Treasury Department in October 2020 highlighted the possibility of sanction breaches that could be associated with ransomware payments to malicious cyber actors.[41] The advisory contains a list of malicious cyber actors sanctioned by the department's Office of Foreign Assets Control, signalling that ransom payments to such actors could be met with civil penalties. Of note, however, is the recognition that 'a company's self-initiated, timely, and complete report of a ransomware attack to law enforcement [will be] a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus'.[42] On this point, a 2019 FBI ransomware alert highlighted the need for ransomware attacks to be reported, regardless of whether money is exchanged.[43] Interestingly, the alert highlights the challenges that affected organisations face—and a possible reticence to prosecute for payment—by stating 'the FBI understands that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers'.[44]

Given that the measures outlined in the Treasury advisory have, to date, not been applied, and the clear focus on reporting and transparency, it could be reasonably concluded in the US that there's little appetite for penalising organisations for paying ransoms. Such a model could be employed in Australia, fostering an information-sharing culture without fear of legal consequences for organisations that pay ransoms. There's also merit in the US approach of publishing a list of known malicious ransomware actors. While that wouldn't remediate the problem, it would serve to better inform organisations about cyber threat actors.

A mandatory reporting regime could take the form of a legal obligation for an organisation to report the nature and root cause of a ransomware attack to the ACSC within a prescribed time frame (for example, within 21 days). That would be in addition to real-time reporting of a cyber incident. Furthermore, this should occur regardless of whether payment is made and ensure the confidentiality of victims. It wouldn't be about naming and shaming. Rather, by compelling victimised organisations to report under law, the ACSC would have improved access to vital and timely intelligence, assisting root-cause analysis and the identification of other attack vectors. Ultimately, when published, this would help better inform other stakeholders on how to reduce vulnerabilities. It would also enhance the operation of the federal government's proposed changes to the *Security of Critical Infrastructure Act 2018*.[45]

It's worth noting recent steps that the European Commission has taken 'to tackle the rising number of serious cyber incidents', announcing on 23 June that it will build a 'Joint Cyber Unit'.[46] The aim of the unit is to provide a coordinated response to 'large-scale' cyber incidents and assist in recovery, operating at both the operational and technical levels.[47] It will involve key stakeholders from law enforcement, security, defence and diplomacy.[48] Its functions will be enhanced by a new US–EU working group, which has been established specifically to address the ransomware threat.[49]

The joint EU and US approach demonstrates that, while Australia can take significant steps to address ransomware domestically by clarifying our law, there's a vital need to work closely with allies and like-minded nations to tackle the threat globally. Longer term, sustained intelligence sharing and the adoption of responsibilities flowing from the agreed UN norms of responsible state behaviour in cyberspace will help achieve international consensus on tackling ransomware.[50] In April, to that end, the Five Eyes nations committed to tackling the growing threat of ransomware, specifically addressing the issue in the Five Country Ministerial Statement Regarding the Threat of Ransomware.[51]

What about cyber insurance?

While still relatively immature, Australia's cyber insurance market has expanded. Cyber insurance policies can be expensive, given the nature of the threat, and broad in scope, covering recovery, replacement and regulatory costs associated with a ransomware attack. Of concern, however, are policies that cover ransom costs, which could serve to encourage attacks targeted at insured entities.[52] There are also concerns that ransomware criminals might access systems in search of insurance certificates and then demand ransom payment of the specific amount covered by an insurer.[53] While there is a role for cyber insurance to play as part of an organisation's holistic cyber security strategy, it is not a silver bullet, and it can have unintended consequences. As noted above, a key risk is the targeting of insured organisations by threat actors. There is also the potential for organisations with cyber insurance to be lax in their approach to managing cyber security. As noted in the Harvard Business Review: "Insurance is important, but it's likely to take a back seat to the broader cyber security discussion...Insurance helps you recover from a situation, filling in the gaps when problems occur that you can't prevent, but attempts to prevent problems are still crucial".

Where do we go from here?

To better protect Australians and their businesses against ransomware, we believe that the three key words are transparency, education and incentivisation.

Increased transparency is vital

As it stands, there's a dearth of official public data relating to ransomware attacks in Australia. For example, and as noted above, in the 2019–20 financial year the ACSC reported an increase in the number of domestic ransomware attacks, but no specific metrics were released.[54] This is in stark contrast to the US, which has a much more transparent reporting system. The FBI publicly reported that it recorded 2,474 ransomware incidents in 2020, amounting to US$29.1 million in economic loss[55] (and that's likely to be a significant understatement of the overall incidence of ransomware attacks because reporting is voluntary).

While it's understandable that the specifics of attacks and victims aren't released into the public domain, if more insight were provided into the prevalence and root causes of ransomware crimes in Australia there would be greater onus on organisations to harden their systems against attack (especially known vulnerabilities). Furthermore, by building a public narrative on the threat landscape and threat actors, policymakers, organisations and the community more broadly would be better informed about the scale of the attacks. This would have a two-pronged effect—encouraging cybersecurity uplift across the economy and enhancing trust in government, especially in the light of the heightened reporting obligations touted for critical infrastructure entities.[56]

In April this year, the US Department of Justice established a dedicated ransomware taskforce. A memo from Acting Deputy Attorney General John Carlin stated that 2020 had been 'the worst year' in history for ransomware and cyber extortion. He signalled that steps would be taken to deal with the root causes of ransomware, which could include actions ranging from ‘takedowns of servers used to spread ransomware to seizures of these criminal enterprises’ ill-gotten gains’.[57]

The US Government’s Cybersecurity and Infrastructure Security Agency (CISA) also provides regular ransomware alerts and tips to the public,[58] which go into significant detail regarding the latest ransomware attacks, the systemic weaknesses that were exploited to gain access for malware to be deployed and steps organisations can take to mitigate those risks. The CISA played a pivotal role in disseminating real-time information about the Colonial Pipeline ransomware attack in May 2021,[59] which brought the major provider of fuel to the US east coast to a grinding halt.[60] The CISA kept the community and critical infrastructure entities informed during what was arguably the most serious ransomware attack the US has seen, ultimately assisting other organisations to be on guard.[61]

The US approach illustrates how comprehensive and more transparent official reporting of ransom ware attacks could be used to enhance preparedness for an attack and people’s understanding of the threat environment. While the ACSC does provide high-level threat intelligence to organisations, there’s a requirement for those organisations to register and be accepted into the ACSC Partnership Program. In addition, the alerts and advice are quite technical, which could make them inaccessible to some organisations, especially small and medium-sized enterprises (SMEs). Hence, there’s a need to build on the existing regime, with a view to enhancing transparency across the entire economy and community via public alerts and advice when ransomware attacks occur.

Education is necessary to improve knowledge and mitigate risk

While increased transparency is vital, it’s of little use if organisations don’t understand what ransomware is, what needs to be done to mitigate risk and haven’t implemented appropriate cybersecurity controls. Many ransomware attacks would be avoidable if effective organisational cybersecurity controls were in place and good cyber hygiene was practised. Ransomware is different from most other tools used by criminals in that it can have far-reaching consequences. The threat it poses through its ability to cripple critical infrastructure makes it all the more serious. Hence, there needs to be greater focus on the basics—a concerted education campaign that explains what ransomware is, what it does and how organisations can bolster their defences.

Top of the list must be patching. Patch management is essential for effective cybersecurity and ensures that the security features of software on computers and devices are up to date. All software is prone to technical vulnerabilities and, when a vulnerability is exposed and shared, cybercriminals have a metaphorical front-door key. A 2019 report by the Ponemon Institute on vulnerability responses found that, of the 48% of organisations that had experienced data breaches in the preceding year, 60% reported that the breaches resulted from failure to patch.[62]

And that brings us to people. Amid the barrage of policies and technical guidance, it’s often forgotten that the route to a cyber breach is surprisingly simple. In most cases, it comes down to a number: 1. That’s the number of people a cybercriminal needs to trick to gain access to a system.

Phishing emails containing malicious links are common lures used to deploy ransomware. The FBI reported 241,342 phishing complaints in 2020 and estimated that phishing cost more than US$54 million.[63] Therefore, training employees to be better prepared to identify suspicious emails—

and not to click on them—is essential. For large, well-resourced organisations, investing in threat hunting is the key.[64] In many cases, the attacker has been inside the victim's network for a significant period, watching and preparing the environment for an attack. An investment in threat hunting means that network anomalies can be more easily recognised and more swiftly contained. It could prove critical in detecting whether a cybercriminal is planning and plotting within a network.

It's the responsibility of all executives, business leaders and boards to be aware of and effectively manage cybersecurity risks, to ensure that appropriate measures are in place and to foster a culture in which cybersecurity really does matter. If cybersecurity matters to a chair and board, that will trickle down and become a priority for the whole organisation. To that end, it's also timely to note that Australian directors increasingly bear personal exposure to cyber risk liability, which may be heightened under the proposed changes to the critical infrastructure regime.

Incentivisation is needed to achieve real cybersecurity uplift

Good cyber hygiene is central to mitigating a ransomware attack, but cybersecurity uplift costs money—a cost that's borne without immediately 'tangible' results for organisations. This is especially pertinent for SMEs, which generally don't have the same level of resourcing to prioritise cybersecurity. Hence, incentivisation has a key role to play if cyber resilience is to be applied across all levels of the economy.

A clear example of where existing mechanisms could be used to incentivise cyber uplift is via full expensing, previously known as instant asset write-offs. The temporary full expensing scheme, which was extended in the 2021–22 federal Budget, allows organisations with an annual turnover of less than $5 billion to immediately write off the business portion of the cost of eligible new assets they first use or install by 30 June 2023, with no cap on the value of new assets that can be claimed (but there may be certain cost limits on particular assets).[65] Put simply, this means organisations can make full or significant deductions for eligible purchases up front, rather than over a period of several years via depreciation. While this doesn't remove the need for initial outlays, the scheme does offer significant taxation benefits. There's clear scope for the federal government to provide clear information via the Australian Taxation Office about what cybersecurity asset purchases are covered under the scheme. As it stands, cybersecurity assets aren't clearly defined, and only bespoke in-house software is covered.[66] If the scheme were broadened to include off-the-shelf products and subscription services (such as cloud services), it would support scalable and more rapid uplift. This relatively simple incentivisation solution, which should be promoted, would have a two-pronged effect, simultaneously easing financial imposts on organisations while also hardening cybersecurity resilience across a greater cross-section of the economy.

Another option is to leverage the power of federal government procurement to drive organisational cybersecurity uplift by mandating minimum cybersecurity standards for organisations feeding into the government supply chain. This has the potential to be transformative, given the government's huge procurement spend (81,174 contracts with a combined value of $53.9 billion were published on AusTender in 2019–20).[67] Despite that massive spend, cybersecurity is mentioned only once in the *Commonwealth Procurement Rules*, [68] which recommend that cybersecurity risk be considered along with other risks and be evaluated in accordance with the government's *Protective Security*

Policy Framework.[69] Cybersecurity needs to play a more prominent role in government procurement practices, not be viewed as an afterthought or secondary consideration. The important role government procurement could play in cyber uplift was highlighted by Rajiv Shah in his 2020 report *Working smarter, not harder*.[70] Shah observed that the government:

> … has an opportunity to leverage its market power to provide for broader benefits to the Australian economy and society … Setting security standards expected from its suppliers may help to lift standards across the board. Companies will be incentivised to lift their standards in order to qualify to do business with the government, and it will often be easier for them to apply those standards across their whole enterprises rather than just for their government contracts.[71]

A cybersecurity uplift grant or subsidy scheme could be considered, in the vein of a program such as the Skilling Australia's Defence Industry Grants Program.[72] That program provides grants to SMEs with fewer than 200 employees over three years, assisting the development of defence sector skills and human resources practices and training plans. The program provides SMEs that service, or intend to service, the defence industry with the capacity and skills required to operate in that supply chain. A similar program could be introduced for organisations that feed into the whole-of-government supply chain to uplift cybersecurity resilience via both training and physical upgrades.

Another option could be to expand and extend the remit of the Cyber Security Business Connect and Protect Program beyond assistance and advice to also include financial aid to lift SME cybersecurity. As it stands, the program (which is currently closed), provides funding to 'trusted organisations' to raise awareness of cybersecurity risks to SMEs, promote action to address those risks and support and lift the cyber capability of SMEs. However, the scheme doesn't provide funding to assist SMEs in the physical implementation of cybersecurity uplift.

Policy recommendations

We make eight policy recommendations under the following themes.

Legal clarity

1. The Australian Government shouldn't criminalise the payment of ransoms. Instead, a mandatory reporting regime should be adopted, fostering an information-sharing culture without fear of legal repercussions.
2. A dedicated cross-departmental ransomware taskforce, including state and territory representatives, should be established to share threat intelligence and develop federal-level policy proposals to tackle ransomware nationally.

Greater transparency

3. The ACSC's existing official alert system should be expanded to include the real-time distribution of publicly available alerts and clear, actionable advice when ransomware attacks are reported. The alerts and advice should be updated as required.
4. The non-punitive mandatory reporting regime should require organisations to report ransomware incidents and known root causes to the ACSC within 21 days. The information would then be de-identified and distributed publicly.
5. The ACSC should publish a list of ransomware threat actors and aliases, giving details of their *modus operandi* and key target sectors, along with suggested mitigation methods.

Low-hanging fruit: incentivisation and education

6. The federal government should implement practical incentivisation measures to drive cybersecurity uplift across the economy via temporary full expensing and changes to procurement practices and grant or subsidy programs.
7. The government should deliver a concerted nationwide public ransomware education campaign, led by the ACSC, across all media. The campaign should highlight the key causes of ransomware vulnerability and how organisations can bolster their security, and it should draw in external expertise where necessary.
8. A business-focussed multi-media public education campaign, led by the ACSC, should be launched to educate organisations of all sizes and their people about basic cybersecurity and cyber hygiene. It should focus on the key areas of patching, multifactor authentication, legacy technology and human error.

Conclusion

Ransomware isn't an abstract possibility. In Australia, the threat's right here, right now and isn't going away. Unless a concerted effort is made to mitigate the risk, the problem could continue to get worse.

There's a key role for the Australian Government to play in leading the way, but tackling ransomware is a shared responsibility. While there's no doubt that organisations must take responsibility for ensuring that their cybersecurity posture is up to scratch, there are practical and easily implementable steps the government can take to provide clarity, guidance and support.

The ongoing ransomware attacks that continue to strike unabated around the world must act as a red flag. And, because we've been warned, we need a plan.

Notes

[1] 'New McAfee report estimates global cybercrime losses to exceed $1 trillion', news release, McAfee, 7 December 2020, online.

[2] Australian Signals Directorate (ASD), 'Ransomware', Australian Government, no date, online.

[3] Cryptocurrency is digital currency secured by cryptography and based on blockchain technology. Cyber Security Industry Advisory Committee (CSIAC), *Locked out: tackling Australia's ransomware threat*, Department of Home Affairs, Australian Government, March 2021, 3, online.

[4] CSIAC, *Locked out: tackling Australia's ransomware threat*, 3.

[5] Edvardas Mikalauskas, 'Report: buying your own malware has never been easier', *Cybernews*, 28 April 2020, online.

[6] Mikalauskas, 'Report: buying your own malware has never been easier'.

[7] Federal Bureau of Investigation (FBI), *Internet crime report 2020*, US Government, 2020, 14. online.

[8] FBI, *Internet crime report 2020*, 14.

[9] FBI, *Internet crime report 2020*, 14.

[10] ASD, *Ransomware in Australia*, Australian Government, October 2020, 1, online.

[11] ASD, *Ransomware in Australia*, 5.

[12] ASD, *Ransomware in Australia*, 4.

[13] Natasha Kassam, 'Safety, security and threats to Australia's vital interests', *Lowy Institute Poll 2021*, Lowy Institute, Sydney, 23 June 2021, online.

[14] Dean Blake, 'Toll customer data stolen in its second cyber attack of 2020', *Inside Retail*, 13 May 2020, online.

[15] Casey Tonkin, 'Toll Group data dumped on dark web: 200GB of files stolen by ransomware group', *Information Age*, 21 May 2020, online.

[16] Paul Smith, 'Hacked again: Toll Group systems hit by fresh ransomware attack', *Australian Financial Review*, 5 May 2020, online.

[17] CSIAC, *Locked out: tackling Australia's ransomware threat*, 10.

[18] Jessica Clifford, 'BlueScope Steel hit by cyber attack causing worldwide system shutdown of operations', *ABC News*, 15 May 2020, online.

[19] Joshua Becker, 'Cyber attack halts Lion production of milk and beer', *ABC News*, 11 June 2020, online.

[20] Ben Grubb, 'Hackers post evidence they have beer giant Lion's confidential files', *Sydney Morning Herald*, 19 June 2020, online.

[21] 'Who we are', Law in Order, 2021, online.

[22] Ronald Mizen, 'Hackers threaten to publish data from attack on legal services firm', *Australian Financial Review*, 24 November 2020, online.

[23] Ry Crozier, 'Nine Entertainment warns ransomware recovery "will take time"', *IT News*, 29 March 2021, online.

[24] Sophie Elsworth, 'Nine Entertainment's cyber attack woes continue to disrupt the media giant', *The Australian*, 5 April 2021, online.

[25] Melissa Cunningham, 'Staff unable to access patient files after Eastern Health cyber attack', *The Age*, 29 March 2021, online.

[26] Rory Callinan, 'UnitingCare cyber attack claimed by notorious ransom gang REvil/Sodin', *ABC News*, 6 May 2021, online.

[27] 'FBI investigating JBS cyber attack that disrupted Australian meat and livestock industry', *ABC News*, 2 June 2021, online.

[28] Ry Crozier, 'JBS Foods pays $14m to ransomware attackers', *IT News*, 10 June 2021, online.

[29] Jack Brewster, 'US recoups "millions" in cryptocurrency ransom paid to Colonial Pipeline hackers', *Forbes*, 7 June 2021, online.

[30] Department of the Treasury, *The American Families Plan tax compliance agenda,* US Government, May 2021, 21, online.

[31] MintDice, 'KYC and AML: how it applies to bitcoin in the USA', *Medium*, 29 November 2020, online.

[32] AUSTRAC, 'New Australian laws to regulate cryptocurrency providers', news release, Australian Government, 11 April 2018, online.

[33] AUSTRAC, 'New Australian laws to regulate cryptocurrency providers'.

[34] ASD, *Ransomware in Australia*.

[35] Sections 400.3–400.8, *Criminal Code Act 1995* (Cwlth).

[36] Section 400.9, *Criminal Code Act 1995* (Cwlth).

[37] Part 5: 27–28, *Charter of the United Nations Act 1945* (Cwlth).

[38] UN, *UN Security Council Consolidated List*, online.

[39] Section 10.2, *Criminal Code Act 1995* (Cwlth).

[40] FBI, *Internet crime report 2020*, 3.

[41] Department of the Treasury, 'Advisory on potential sanctions risks for facilitating ransomware payments', US Government, 1 October 2020, 1, online.

[42] Department of the Treasury, 'Advisory on potential sanctions risks for facilitating ransomware payments', 4.

[43] FBI, 'High-impact ransomware attacks threaten US businesses and organizations', alert no. I-100219-PSA, US Government, 2 October 2019, online.

[44] FBI, 'High-impact ransomware attacks threaten US businesses and organizations'.

[45] Department of Home Affairs (DHA), 'Protecting critical infrastructure and systems of national significance: Security Legislation Amendment (Critical Infrastructure) Bill 2020', Australian Government, 2020, online.

[46] European Commission (EC), 'EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents', press release, 23 June 2021, online.

[47] EC, 'EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents'.

[48] EC, 'Factsheet Joint Cyber Unit', 23 June 2021, online.

49 Laurens Cerulus, Clothilde Goujard, ‘EU, US launch initiative against ransomware’, *Politico*, 22 June 2021, online.

50 https://www.aspi.org.au/cybernorms; https://ad-aspi.s3-ap-southeast-2.amazonaws.com/2020-09/cybernorms_ENGLISH.mp4

51 ‘Five Country Ministerial Statement Regarding the Threat of Ransomware’, 7–8 April 2021, online.

52 CSIAC, *Locked out: tackling Australia’s ransomware threat*, 9.

53 Alicia Hope, ‘Cyber insurance firm suffers sophisticated ransomware cyber attack; data obtained may help hackers better target firm’s customers’, *CPO Magazine*, 5 April 2021, online.

54 ASD, *Ransomware in Australia*, 1.

55 FBI, *Internet crime report 2020*, 3.

56 DHA, ‘Protecting critical infrastructure and systems of national significance: Security Legislation Amendment (Critical Infrastructure) Bill 2020’.

57 Charlie Osborne, ‘New US Justice Department team aims to disrupt ransomware operations’, *ZDNet*, 22 April 2021, online.

58 Cybersecurity & Infrastructure Security Agency (CISA), ‘Ransomware alerts and tips’, US Government, 2021, online.

59 CISA, ‘DarkSide ransomware: best practices for preventing business disruption from ransomware attacks’, alert AA21-131a, US Government, 11 May 2021, online.

60 Mary-Ann Russon, ‘US fuel pipeline hackers “didn’t mean to create problems”’, *BBC News*, 10 May 2021, online.

61 ‘Government races to secure critical infrastructure in wake of Colonial Pipeline ransomware attack’, National Law Review, 3 July 2021, online.

62 Ponemon Institute LLC, *Costs and consequences of gaps in vulnerability response*, ServiceNow, no date, online, P5.

63 FBI, *Internet crime report 2020*, 3.

64 CrowdStrike, *2021 global threat report*, 2021, 50, online.

65 Michael Janda, ‘Federal budget leaves business owners smiling as instant investment tax breaks extended’, *ABC News*, 13 May 2021, online.

66 Australian Taxation Office, ‘In-house software’, Australian Government, 23 April 2019, online.

67 Department of Finance, ‘Procurement’, Australian Government, no date, online.

68 Department of Finance, *Commonwealth Procurement Rules*, Australian Government, 14 December 2020, 20, online, P20.

69 Attorney-General’s Department, ‘The Protective Security Policy Framework’, Australian Government, no date, online.

70 Rajiv Shah, *Working smarter, not harder: leveraging government procurement to improve cybersecurity and supply chains*, ASPI, Canberra, 18 August 2020, online.

71 Shah, *Working smarter, not harder: leveraging government procurement to improve cybersecurity and supply chains.*

72 ‘Current grant opportunity view—GO4147’, *GrantConnect*, Australian Government, 4 September 2020, online.

Acronyms and abbreviations

ACSC	Australian Cyber Security Centre
AML	anti-money-laundering
CISA	Cybersecurity and Infrastructure Security Agency (US)
EU	European Union
FBI	Federal Bureau of Investigation (US)
KYC	know your customer
SMEs	small and medium-sized enterprises

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

INTERNATIONAL
CYBER POLICY
CENTRE

TWENTY YEARS OF ASPI STRATEGY
2001 - 2021