MAY 2023

Combatting Ransomware

Policy Paper

PREPARED BY PROFESSOR JOHANNA WEAVER, TANVI NAIR AND LEAH LAFFERTY

Combatting Ransomware by starryai

Introduction

The Optus,[ii] Medibank,[iii] and Latitude Financial[iv] cyber incidents catapulted ransomware into the headlines and public consciousness in Australia.

While the threat is not novel, the occurrence of these three high-profile cyber incidents in quick succession created a palpable demand from the public and industry for the government to act.

Responding to that demand, this paper details seven actionable policy options available to the Australian government to combat ransomware.

We recommend the adoption of a clear policy *against* payment of ransoms but do not support a complete ban or criminalisation of ransom payments (as it shifts the burden of breaking the ransomware business model to the victim).

Australia's forthcoming Cyber Security Strategy provides an opportunity to recalibrate Australia's policy settings. The upcoming Quad Leaders' Summit in Sydney on 24 May 2023 is also an opportunity for the governments of Australia, India, Japan, and the United States to commit to collective action against this global threat. Australia's leadership of the International Counter Ransomware Taskforce is another ongoing opportunity to galvanise action across the 37 member states of the Counter Ransomware Initiative. Recommendations are therefore divided into actions for Quad and actions for Australia and broader like-minded partners.

Recommendations

Quad should:

1. Condemn the activities of ransomware criminals and articulate a joint policy position strongly discouraging payment of ransoms.

2. Introduce common mandatory disclosure requirements compelling entities that pay ransoms to confidentially notify an appropriate authority within 24 hours of the decision to pay.

3. Harmonise cyber incident reporting across Quad jurisdictions.

Australia should:

4. Introduce annual Cyber Resilience Board Statements for ASX-listed companies.

5. Establish a cyber insurance taskforce (under the National Cabinet) to examine means for the cyber-insurance market to incentivise cyber resilience and reduce the impact of ransomware.

6. Sanction individuals and entities most prolifically conducting significant ransomware incidents, in close coordination with like-minded countries.

7. Step-up international engagement to combat ransomware, especially vis-a-vis 'safe haven' states, in close coordination with like-minded countries.

> *"Ransomware is the most destructive cybercrime threat. All sectors of the Australian economy were directly impacted by ransomware in the last financial year."*
>
> **– Australian Cyber Security Centre Annual Threat Report (2022)**

Methodology

The recommendations in this paper were informed by independent research and analysis, and discussions at an executive workshop.

The workshop was hosted by the ANU Tech Policy Design Centre (TPDC) on 27 April 2023 and attended by 44 senior representatives of industry groups, companies, government, and academia. A list of organisations is at Annex A.

During the workshop, participants were first asked to reflect on a set of fictitious scenarios (Annex B) some of which were extrapolated from global cyber incidents. Participants indicated via an anonymous survey when they would condone the payment of a ransom. Of the 44 workshop participants, 18 returned the survey, the results of which are collated in Figure 1. All workshop participants engaged in discussions centred on the scenarios.

After the scenario exercise, TPDC facilitated a discussion on each of the questions posed in the discussion paper prepared by TPDC (Annex C).

Following the workshop, TPDC conducted further research and analysis.

The discussion section below indicates when observations reflect the majority views of workshop participants. In all other instances, this paper, including its recommendations, reflect the independent views of TPDC.

To Pay or Not to Pay

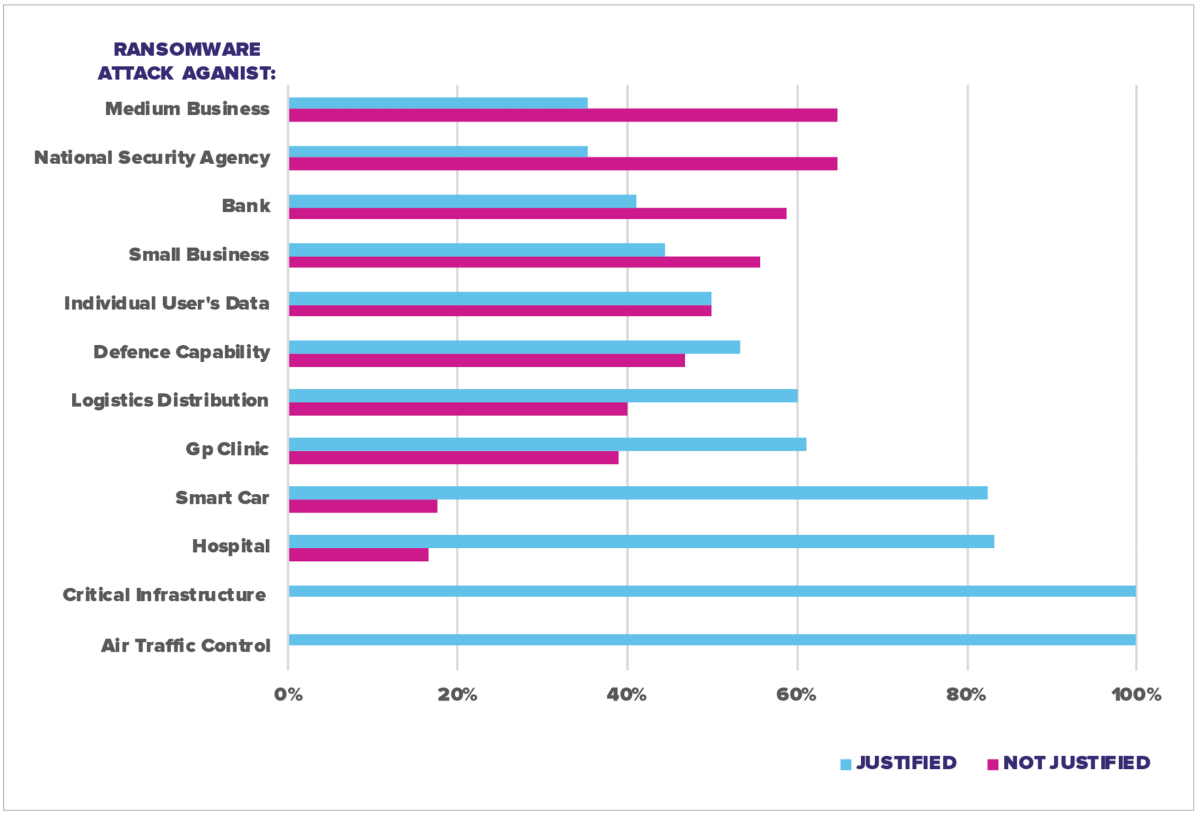


Figure 1: Executive workshop participants' responses (n=18) to scenarios positing when the payment of ransoms may be justified. The scenarios are included in Annex B.

Discussion

Recommendation 1: Quad should condemn the activities of ransomware criminals and articulate a joint policy position strongly discouraging payment of ransoms.

There was general agreement among workshop participants that government should articulate a clear policy position against the payment of ransoms. There was, however, little or no support for a total ban or the criminalisation of payment of ransoms.

Workshop participants emphasised the need to set a clear expectation that ransoms should not be paid. However, they equally emphasised the importance of recognising that – in exceptional circumstances – payment may be the best of a bad set of options.

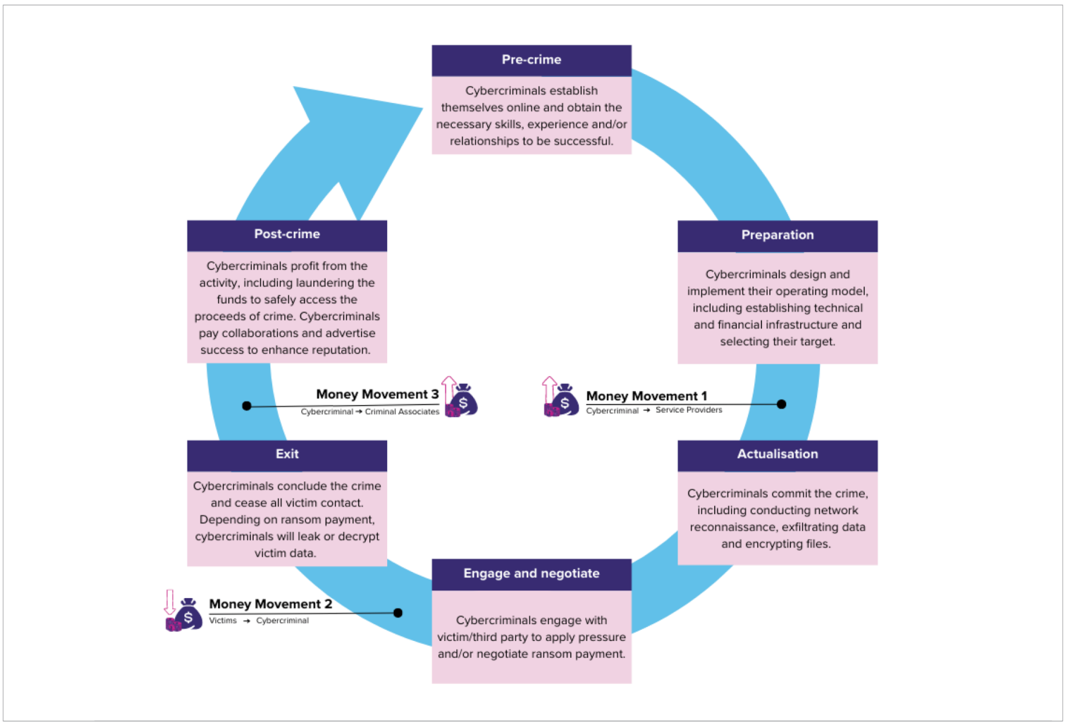
For example, as represented in Figure 1 above, workshop participants condoned payment of a ransom when there was an imminent threat to multiple lives, or in the case of interruption to critical services resulting in civil unrest.

To reiterate, the default position was that ransoms should not be paid. However, the scenario discussions underscored the need for a nuanced case-by-case assessment.

There was also concern that a blanket ban would drive payments further underground, deter incident reporting, and decrease the visibility of the true extent and impact of the crime.

Breaking the ransomware business model was recognised as a laudable objective. However, the prevailing view of workshop participants was that criminalising the payment of ransoms unfairly shifted the burden of breaking the ransomware business model to the victim of the crime and focused too narrowly on a single element of the ransomware business model (specifically Money Movement 2, depicted in Figure 2 below).

Ransomware Business Model



Cybercriminals establish themselves online and obtain the necessary skills, experience and/or relationships to be successful.

Cybercriminals design and implement their operating model, including establishing technical and financial infrastructure and selecting their target.

Cybercriminals commit the crime, including conducting network reconnaissance, exfiltrating data and encrypting files.

Cybercriminals engage with victim/third party to apply pressure and/or negotiate ransom payment.

Cybercriminals conclude the crime and cease all victim contact. Depending on ransom payment, cybercriminals will leak or decrypt victim data.

Cybercriminals profit from the activity, including laundering the funds to safely access the proceeds of crime. Cybercriminals pay collaborations and advertise success to enhance reputation.

Figure 2: Ransomware Business Model – from Australian Cyber Security Centre Annual Threat Report (2022).

Recommendation 2: Quad should introduce common mandatory disclosure requirements compelling entities that pay ransoms to confidentially notify an appropriate authority within 24 hours of the decision to pay.

Payment of ransoms should occur by exception (see Recommendation 1). When ransoms are paid, information about the payments (who was paid, by what means, and how much) will improve evidence-based analysis of trends. In turn, this disclosure will enhance mitigations, inform law enforcement activities, and allow for better assessment of the effectiveness of policy changes.

The was strong support among workshop participants for safe harbour protections to be built in (that is, any information obtained as the sole result of the disclosure should not be admissible in evidence against the entity).

While a small number of workshop participants argued for public disclosure, a majority supported confidential disclosure to the relevant government agency (in Australia, this would be either the Australian Cyber Security Centre or the Department of Home Affairs). There was strong support for collated, anonymised datasets to be made publicly available. This will improve public awareness of and inform independent research into the ransomware ecosystem.

Recommendation 3: Quad should harmonise cyber incident reporting across Quad jurisdictions.

Quad countries have vastly different mandatory reporting requirements for cyber incidents (see Table 1 below).

The unique circumstances and priorities across jurisdictions make absolute harmonisation challenging. However, there was strong support among workshop participants for Quad to develop a common set of minimum reporting requirements (adequacy) and automate sharing of incident reports and distribution of the same via respective domestic threat-sharing platforms.

Adequacy and automation will allow Quad governments to mutually recognise reporting (equivalency), minimising the reporting burden on victims, while maximising threat sharing at scale in real-time.

Well-established cyber incident sharing protocols should be applied to ensure appropriate protection and de-identification of data. As with Recommendation 2, collated, anonymised datasets should be made publicly available.

Minimum reporting requirements should clarify which types of ransomware incidents should be reported. It would be valuable not just to capture ransom payments (Recommendation 2) but also lessons learnt from organisations that do not pay a ransom and successfully recover.

Table 1: Overview of Quad Cyber Incident Reporting Requirements

**Excludes breach notification requirements provided for privacy or data protection*

	Entities that Must Report Breaches	Timeframe to Report Breaches	Report to:	Related Legislation
Australia	Critical infrastructure sectors and assets Telecommunications Carriers and Carriage Service Providers	**12 hours:** • Any critical cyber security incident: that has had or is having a significant impact on the availability of the asset. **72 hours:** • Any other cyber security incident: has had, is having or is likely to have a relevant impact on the asset. **Note:** Systems of National Significance may also be subject to additional reporting requirements if directed in a Systems Information Notice issued by the Secretary of the Department of Home Affairs.	Australian Cyber Security Centre (ACSC)	*Security of Critical Infrastructure Act 2018* *Security Legislation Amendment (Critical Infrastructure) Act 2021* *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* *Telecommunications (Carrier License Conditions – Security Information) Declaration 2022* *Telecommunications (Carriage Service Provider – Security Information) Determination 2022*
India	Any service provider, intermediary, data centre, body corporate and Government organisation	**6 hours:** • Any cyber security incident	Indian Computer Emergency Response Team (CERT-IN)	*The Information Technology Act 2000* *IT Act 2000, Section 70B* *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*
Japan	Telecommunications carriers	**30 days:** • A cyber-attack that causes a serious incident	Ministry of Information Communications (MIC)	*The Telecommunications Business Act (TBA)*
United States	Federal civilian agencies	**72 hours:** • A 'substantial' cyber incident **24 hours:** • A ransom payment	Cybersecurity and Infrastructure Security Agency (CISA)	*Strengthening American Cybersecurity Act of 2022*
	Businesses that own or manage critical infrastructure	**72 hours:** • A cyber security incident **24 hours:** • A ransom payment	Cybersecurity and Infrastructure Security Agency (CISA)	*Cyber Incident Reporting for Critical Infrastructure Act 2022*

Recommendation 4: Australia should introduce annual Cyber Resilience Board Statements for ASX-listed companies.

There was strong support among workshop participants for the introduction of annual Cyber Resilience Board Statements. Such a compliance model would help drive the cultural change needed to prioritise cyber security maturity.

Accountability at the board level is a feature of Australia's *Modern Slavery Act (2018)*, which requires boards to report on actions taken to address risks of slavery in supply chains. That Act is often criticised for a lack of penalties and enforcement,[v] but it has indisputably directed board-level attention to the issue of modern slavery and set a public expectation of corporate behaviour.

Workshop participants underscored that any such obligation would need to be carefully calibrated to ensure that boards were not obligated to disclose vulnerabilities that increase targeting by malicious actors. The focus should be on fostering cyber resilience, not tick-box compliance.

Workshop participants also emphasised that cyber resilience should be broadly construed. For example, statements should capture expenditure on the replacement of legacy equipment, which generally is not allocated against the cyber security budget, but has a direct impact on cyber resilience.

Recommendation 5: Australia should establish a cyber insurance taskforce (under the National Cabinet) to examine means for the cyber insurance market to incentivise cyber resilience and reduce the impact of ransomware.

There was general agreement among workshop participants that cyber insurance could play an important role in incentivising better cyber security practices and reducing impacts on ransomware victims. That said, there was consensus that cyber insurance did not currently play this role.

This is not the first instance of the insurance industry having trouble incentivising and establishing a clear market. One participant gave the example of the late 1990's early 2000's when Australian Federal and State and Territory Governments acted in concert to reduce the cost of professional indemnity insurance.

The Australian National Cabinet should establish a taskforce to examine means for the cyber insurance market to incentivise cyber resilience and reduce the impact of ransomware. For example, this could include establishing a mechanism whereby, if entities can demonstrate good cyber security against agreed standards, liability could be capped and premiums for cyber insurance reduced, thereby creating a more viable market for insurance while lifting the bar on cyber resilience.

Recommendation 6: Australia should sanction individuals and entities most prolifically conducting significant ransomware incidents, in close coordination with like-minded countries.

Australia introduced a Significant Cyber Incidents Sanctions Regime in 2021,[vi] but is yet to be used. There was general agreement among workshop participants that the regime should be activated, in concert with like-minded partners.

While it would never be possible to sanction all malicious actors, the deterrent effect of targeted sanctions should not be underestimated. The effect of sanctions is to prohibit the transfer of funds to sanctioned entities or individuals; it is, therefore a nuanced means to ban the payment of ransoms to the *most prolific* malicious actors that conduct the *most significant* incidents.

Workshop participants emphasised that identifying ransomware payment recipients can be challenging, and even sometimes politicised. Therefore, it is important for the government to set out clear due diligence requirements and ensure that the public is informed of them.

Timely imposition of sanctions in coordination with like-minded partners would increase the impact of sanctions. This would require rapid and public attribution, necessitating capability investment by the Australian government and enhanced collaboration with international partners.

Sanctions should complement, but not replace, law enforcement activities.

Recommendation 7: Australian should step-up international engagement to combat ransomware, especially vis-a-vis 'safe haven' states, in close coordination with like-minded countries.

'Safe haven' states are jurisdictions where ransomware actors operate with impunity due to a) explicit state protection or wilful blindness towards the activities of ransomware groups, or b) a lack of capacity to respond.

For states that overtly or covertly condone the activities of ransomware groups, there was support among workshop participants for the Quad or other like-minded countries to exert pressure for these states to combat ransomware attacks emanating from their jurisdictions. This could include implementing economic and trade sanctions, "naming and shaming" in public forums, withholding military or foreign aid, or denying visas to citizens.

Quad and other like-minded countries could deliver training, adopt capacity-building programmes, and undertake joint law enforcement operations to address ransomware attacks originating from 'safe haven' states that do not have adequate resources to independently investigate or prosecute ransomware groups.

It is important to be mindful of states' capacity to absorb this type of cooperation and to ensure that the cooperation responds to a specific need or request from the recovering state. Australia, Quad and like-minded states should better coordinate – our collective efforts should complement, not compete.

Annex A – List of Organisations Represented at the Executive Workshop

Government

- Australian Prudential Regulation Authority
- Attorney-General's Department
- Australian Federal Police
- Department of Home Affairs

Industry Associations

- Australian Industry Group
- Australian Information Industry Association
- Australian Institute of Company Directors
- Australian Security Policy Institute
- Business Council of Australia
- Tech Council of Australia

Industry

- Atlassian*
- AUCloud
- AWS
- BlackBerry
- Cisco
- CyberCX
- Datacom
- IBM
- Microsoft (Australia)
- Microsoft (Singapore)
- NBN Co
- PwC
- Seek
- SentinelOne
- Verizon
- Woolworths

Academia and Think Tanks

- Australian National University
  - College of Computing, Engineering and Cybernetics
  - College of Law
  - National Security College
  - Office of the Chief Information Security Officer
  - Tech Policy Design Centre
- Australian Strategic Policy Institute
- University College London

Note 1: *to encourage frank discussions, participants at the executive workshop were given the option not to be included in this list. Several organisations took up this option.*

Note 2: *while informed by the discussions at the executive workshop, the recommendations of this paper represent the independent views of TPDC.*

Note 3: **did not attend the workshop; provided written comments on the discussion paper.*

Annex B – Workshop Scenarios

Combatting Ransomware Scenarios

This paper provides fictional scenarios to provoke discussion with a view to mapping out the contours of when it may be considered acceptable to pay a ransom.

Scenario 1: Individual User's Data

An individual finds that most of the functions on their personal computer have stopped working. They can't do anything on their laptop, except respond to a mysterious email that demands payment in cryptocurrency to unlock the computer. The computer contains all their family photos and the first draft of a novel. No backups are held.

Scenario 2: Small Business

One day, an owner of a small candle-making store notices that they can't access any of their files on the computer to process payments and review stock. The business operates on a week-to-week cash flow basis. They receive an email demanding a payment in cryptocurrency to unlock the files. They have not backed up these files. If they are deleted, the owner will not be able to recover them.

Scenario 3: GP Clinic

Returning to work after a long weekend, the receptionist at a GP Clinic becomes aware that the clinic has been the subject of a ransomware attack. Phones, payments, bookings, patient records, and prescriptions are inaccessible. The clinic manager contacts their MSP to activate the offsite backup but is advised that, due to a glitch, the backup is inaccessible and there is no way to retrieve data.

Scenario 4: Medium Business

A medium company responsible for providing the online platform for psychological testing in job applications reported a large data breach that affected millions of users. The hackers demand payment in cryptocurrency, otherwise, they will leak users' sensitive personal data online. The computer systems can be restored from backup, but the ransomware group holds the stolen data. For every hour that passes, hundreds of user data is released on the dark web.

Scenario 5: Hospital

A hospital finds that they can't access any of their ER computers; they cannot process new patients or appointments, fix billing, or access lab reports. Hospital operations have come to a standstill, and they are struggling to keep up with the demand of patients who need urgent medical attention. Shortly after, another hospital in the area also reports the same problem. The hospital system is quickly becoming overwhelmed. One hacker group is taking credit for both attacks, threatens to attack more hospitals, and demands payment in cryptocurrency to unlock the systems.

Scenario 6: Bank

A bank reports that there has been a breach in their system and that the sensitive personal data of thousands of their clients was stolen. The integrity and availability of the banking system remain otherwise intact. The attackers have demanded payment in cryptocurrency, or they will release the personal sensitive data of these clients on the dark web. The AFP confirms that the attackers have already released the information of a hundred clients, including individuals in witness protection.

Scenario 7: Critical Infrastructure

In the middle of summer of record-breaking heat waves, residents of a large city wake up to no electricity. Workers on the main electricity provider find that they have been locked out of the computer system that manages distribution through the grid. The barometer is raising, deaths from health stroke are already being reported in nursing homes, and hospitals are struggling to maintain emergency operations in generator systems. Supermarkets are struggling to keep fridges operational. Residents are becoming panicked; the risk of civil unrest is rising with the temperature. The CI provider believes it can restore the system, but it will take at least a week.

Scenario 8: Smart Car

A driver with a smart electric car realises that the touchscreen of the car isn't working. It then dawns that they had lost all ability to control the car and could not brake or steer the vehicle. The individual receives a message on their phone with a link demanding that they pay in cryptocurrency to regain access to the car. The car is approaching a school zone during school pick-up.

Scenario 9: Air Traffic Control

During a storm computer screens in the Air Traffic Control tower at Australia's busiest airport go blank, then flash with a ransom demand. Quickly activating emergency plans, traffic controllers use analogue phones to ask colleagues at the nominated alternate airport to advise planes to remain in storm holding patterns, alleviating potential in-air collisions. Due to the storm, many planes are running low on fuel. Via a relayed message the tower and pilots begin to map out which planes are where in the air. It quickly becomes apparent that several planes risk running out of fuel and crashing if the computer system is not restored.

Scenario 10: National Security Agency

A government employee working in the intelligence community clicks on a link from an external email. They find that they can't access any of their documents, including on the 'air-gapped' classified system. Soon, multiple employees from the agency start complaining that they can't access any of their files either. The attackers demand payment in cryptocurrency be transferred to them, threatening that they would start publishing the information from the files. The attackers begin releasing files containing classified national security information onto the dark web.

Scenario 11: Logistics Distribution

The platform used by 87 per cent of Australian logistics companies is subject to a ransomware attack. Freight and interstate transport grind to a halt. Cyber security experts and the IT company are working around the clock to get a replacement system based on restored backups, without success. Food, fuel, medicine, and toilet paper stocks are quickly running low. There is a rush in supermarkets. The Prime Minister calls for calm.

Scenario 12: Defence Capability

Engineers building a new submarine with technologies shared by other countries find that the files relating to the design are missing from their systems. All plans, including minutia details on how to build the submarine and what technology is needed, are missing. The department the engineers work for gets an email from the hacker demanding that cryptocurrency must be paid to restore access to the files, promising to delete any copies. The department knows that at risk is Australia's national security and the loss of trust in an important strategic partner.

Annex B – Discussion Paper

Combatting Ransomware: Policy Options

This discussion paper provides seven potential policy options to combat ransomware. Each will be discussed and stress-tested at the workshop on 27 April for government and industry senior executives, hosted by the ANU Tech Policy Design Centre in partnership with Microsoft.

The intent of the workshop is to develop a set of actionable recommendations to inform the implementation of the Quad Foreign Ministers' Statement on Ransomware. The policy options are equally relevant to the International Counter Ransomware Task Force (led by Australia under the US-led Counter Ransomware Initiative, comprised of 37 like-minded governments), and to Australia's Cyber Security Strategy review. To contribute additional options for consideration at the workshop please email: techpolicydesign@anu.edu.au

1. Banning Ransomware Payments/Disclosure of Ransomware Payments

If Quad countries collectively banned ransomware payments it would significantly interrupt the ransomware business model. Conversely, however, if a ransom is not paid, and the incident cannot be mitigated quickly, ransomware incidents could interrupt the delivery of critical services to the public. **Does your organisation support a ban on ransomware payments? If not, in what circumstances does your organisation consider it would be acceptable to pay a ransom?**

As an alternative to an outright ban, or as an interim step towards such a ban, Quad countries could require entities that pay ransoms to disclose those payments (publicly, or to relevant government agencies) within 24 hours of payment. A freeze on regulator investigations (during immediate incident management) and safe havens from prosecution warrant consideration. The costs and benefits of public and confidential disclosure also need to be considered. Confidential disclosure would offset the risk of increased targeting of victims; privacy concerns; compliance burden; and reputational risk for victims. Whereas the prospect of public disclosure could motivate entities to proactively uplift cyber security capability. **Does your organisation support a disclosure obligation? If yes, is public or confidential disclosure preferred? What is your position on the need for investigation freezes and prosecution safe harbours?**

2. Cyber Sanctions

As another alternative to an outright ban on ransomware payments, Quad countries could impose coordinated cyber sanctions on individuals or groups that target critical infrastructure. In effect, this would limit monetary gain from ransomware attacks (as it is illegal to transfer funds to sanctioned entities or individuals) and discourage ransomware targeting critical infrastructure (the potential impact of which is most significant). This would require rapid and public attribution, which may require capability investment by government(s). Coordinated and timely imposition of sanctions would increase the impact. Effective communication with the private sector and clear due diligence guidelines would need to be developed. **Does your organisation support the targeted imposition of cyber sanctions? If yes, should such sanctions be limited to entities or individuals that target critical infrastructure?**

3. Cyber Insurance

Cyber insurance is a risk management strategy for cyber incidents, however, not all insurers impose cyber security requirements on beneficiaries. Quad countries could mandate that insurance companies must require minimum cyber security standards to be met before beneficiaries qualify for insurance. This would have flow-on effects, including raising sector-wide cyber security, maturing the cyber insurance industry, and reducing costs incurred ex-post-facto. Regulatory frameworks would need to be developed to enforce any such requirement. Another option could be to prohibit insurance payouts to cover ransomware payments. **Does your organisation support the imposition of minimum cyber security standards on insurance beneficiaries and/or a prohibition on insurance payouts to cover ransomware payments?**

4. Board Compliance Statement on Cybersecurity Hygiene

Separate from Directors' Duties, compliance models, including that outlined in Australia's Modern Slavery Act (2018), could prove instructive in raising cyber security maturity. That Act requires boards to report on actions taken to address risks of slavery in supply chains. Applied to cyber security, boards could issue a statement or addendum to annual reports on actions or budgets allocated to cybersecurity. Some countries already impose similar requirements. Guidance and templates could be developed to harmonise and minimise the compliance burden. Board-directed compliance would enhance transparency while helping to drive the cultural changed need to ensure the appropriate allocation of resources to cyber security. **Does your organisation support a requirement for Board Cyber Security Compliance Statements?**

5. Harmonisation of Reporting on Cyber Breaches Between Quad Countries

Quad countries have vastly different reporting requirements for cyber incidents. Incident reporting could be harmonised between Quad countries, and then like-minded. These standards could be designed to allow for appropriate flexibility for unique circumstances and priorities across jurisdictions. A mechanism for monitoring and evaluation of harmonised reporting standards would enable improved and automated information-sharing, allowing countries to make necessary improvements and adjustments, to better detect, deter, and mitigate ransomware (and other malicious cyber activity). **Does your organisation support the harmonisation of cyber incident reporting requirements across Quad countries?**

6. Exert Pressure on States that Provide 'Safe Havens'

'Safe haven' states are jurisdictions where ransomware actors operate with impunity - this may be due to explicit protection for ransomware criminals, wilful blindness, or a lack of capacity to respond. For states that fall into the first two categories, Quad countries could exert pressure by implementing economic and trade sanctions, "naming and shaming" safe havens states in public forums, withholding military or foreign aid, or denying visas to citizens. For 'Safe haven' states that do not have adequate resources to investigate or prosecute ransomware actors, incentives, rather than punitive measures, may be more impactful. This could include training, capacity-building and joint law enforcement operations. It is important to be mindful of states' capacity to absorb this type of cooperation. Australia, Quad and like-minded should better coordinate – our collective efforts should complement, not compete. **Does your organisation support exerting pressure on safe-haven states?**

7. Quad Collaboration with ASEAN Regional Forum to Deter Ransomware

The ASEAN Regional Forum (ARF) is a key forum for security dialogue and cooperation in the Indo-Pacific region. Australia, the Quad and like-minded ARF members could facilitate discussions on combatting ransomware between ARF member states. This would expand discussions beyond traditional like-minded partners. Note, however, that China, Russia, and North Korea are ARF members. On occasion (especially when it comes to operational matters) the first two can be quietly pragmatic within ARF; however, if issues are perceived to be politicised, it is not unusual for Russia in particular to play a spoiler role. It may therefore be more practical to facilitate cooperation through forums like the ASEAN-Australia Cyber Dialogue. **Does your organisation support regional collaboration to combat ransomware?**

Endnotes

[i] Image was generated using Starryai on 24 May 2023 using the following prompt "*create an image that depicts a gender and race diverse team of cybersecurity experts working together to defeat ransomware attacks. The image should be set outdoors, in the jungle, with lush greenery and vibrant purple accents throughout the scene. The team should be shown sitting at a table or huddled around a laptop, with a sense of teamwork, resilience, and determination evident in their body language and expressions. The experts should be using the latest tools and techniques to identify, isolate, and neutralise ransomware threats. The overall tone of the image should be positive and inspiring, conveying the idea that with the right approach and expertise, ransomware attacks can be overcome and prevented*".

[ii] Singtel Optus Pty Limited, "*Optus Notifies Customers of Cyberattack Compromising Customer Information,*" Press Release, September 22, 2022, http://www.optus.com.au/about/media-centre/media-releases/2022/09/optus-notifies-customers-of-cyberattack

[iii] Emily Ritchie, "*Medibank Cyber Incident*," Press Release, Medibank Newsroom, October 13, 2022, https://www.medibank.com.au/livebetter/newsroom/post/medibank-cyber-incident.

[iii] Latitude Group Holdings Ltd, "*Cyber Incident*," Press Release, March 16, 2023, https://www.latitudefinancial.com.au/about-us/media-releases/latitude-cyber-incident.html.

[iv] Fiona McGaughey et al., "Corporate Responses to Tackling Modern Slavery: A Comparative Analysis of Australia, France and the United Kingdom," *Business and Human Rights Journal 7, no. 2 (June 2022)*: 249–70, https://doi.org/10.1017/bhj.2021.47; Fiona McGaughey, "Behind the Scenes: Reporting under Australia's Modern Slavery Act," *Australian Journal of Human Rights 27, no. 1 (2021)*: 20–39, https://doi.org/10.1080/1323238X.2021.1962788; Ramona Vijeyarasa, "A Missed Opportunity: How Australia Failed to Make Its Modern Slavery Act a Global Example of Good Practice Comments," *Adelaide Law Review 40, no. 3 (2019)*: 857–66.

[v] Department of Foreign Affairs and Trade, "Significant cyber incidents sanctions regime", https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/significant-cyber-incidents-sanctions-regime

About the Tech Policy Design Centre

The Tech Policy Design Centre (TPDC) is a nonpartisan, independent research organisation at the Australian National University. TPDC's mission is to develop fit-for-purpose tech policy frameworks to shape technology for the long-term benefit of humanity. We work to mature the tech-governance ecosystem in collaboration with industry, government, civil society, and academia.

Independence Statement

Our work is made possible by the generous support of external funders from government, industry, and civil society. Our research aligns with ANU's Statement on Academic Freedom. In all instances, TPDC retains full independence over our research and complete editorial discretion with respect to outputs, reports, and recommendations.

Authors

Professor Johanna Weaver, Director, ANU Tech Policy Design Centre

Tanvi Nair, Research Fellow, ANU Tech Policy Design Centre

Leah Lafferty, Research Assistant, ANU Tech Policy Design Centre

With invaluable support from: Dr Harry Rolf, Dr Huon Curtis, Lucy Ryrie, James Jackson and Niamh Healy.

Dedication

This report is dedicated to Tanvi Nair's mother Mini Nair.
Thank you for your unwavering love and encouragement.

Acknowledgements

The ANU TPDC acknowledges the Ngunnawal and Ngambri people, who are the Traditional Owners of the land upon which this report was prepared. We pay our respects to their elders, past and present.

This report was prepared by ANU TPDC, with thanks to generous sponsorship from Microsoft.

TPDC thanks the peer reviewers of this paper: Dr Anton Moiseienko, Dr James Mortenson, and Michael Karimian.

The report's cover was illustrated by starryai, artificial intelligence image generator (see Endnote 1).

Citation

Weaver, J. Nair, T. and Lafferty, L. 2023, Combatting Ransomware, ANU Tech Policy Design Centre, Canberra, ACT.

Contact

Tech Policy Design Centre
Level 4, Building 7
5 Fellows Road
The Australian National University Canberra ACT 2601, Australia
techpolicydesign@anu.edu.au
CRICOS Provider: 00120C

Australian National University

TECH POLICY DESIGN CENTRE

Tech Policy Design Centre
Australian National University

E: techpolicydesign@anu.edu.au
W: www.techpolicydesign.au
TPDesignCentre