Submission on the 2023-2030 Australian Cyber Security Strategy Discussion Paper

I welcome the opportunity to make a submission on the questions posed in the Australian Government's *2023-2030 Australian Cyber Security Strategy Discussion Paper*.

I support the Government's vision of making Australia the most cyber secure country by 2030, and offer my views on the Discussion Paper in this document. Specifically, I have focused my feedback on questions pertaining to the potential prohibition on the payment of ransoms and extortion demands by companies, and have provided my view on the effect this would have on Australian businesses.

I would welcome the opportunity to work with the Government to further the development of this Strategy and to propose practical solutions to the issues identified by the Government.

Kind regards,

Paul Dutkowski

[redacted]

About Me

I am a cyber security and technology risk professional with experience across a broad range of industries including defence, intelligence, mining and metals, oil and gas, and financial services. I have built and assessed information security programs and strategies, assessed the maturity of organisational incident response capabilities, helped build SOCs and CSIRTs, acted as a trusted advisor to C-suite executives and board members, and assisted organisations across the globe with their security transformation.

I have led strategic advisory engagements aimed at helping clients develop their defensive cyber security capabilities, allowing them to better prevent, detect and respond to incidents ranging from commodity malware to targeted state-sponsored intrusions. I have worked with clients across the globe in a wide range of industries, including several ASX 100 and Fortune 500 companies.

I currently work as an independent consultant and advisor. My past employers include [redacted]

My professional qualifications include an MSc (Information Technology), BSc (Computer Science), CISSP, CISM, CRISC, GXPN, GICSP, GPEN, GCIH and GCIA.

Responses

f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: (a) victims of cybercrime; and/or (b) insurers? If so, under what circumstances?

i. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?

No, the Government should not prohibit the payment of ransoms and extortion demands. Prohibiting the payment of ransoms and extortion demands would:

1) Do little to reduce cyber crime in Australia;
2) Destroy many businesses that fall victim to cyber attacks which might otherwise be able to survive by paying a ransom;
3) Cause significant harm to businesses who could recover operations only after a lengthy process;
4) Limit the options available to victims of cyber crime without providing them with any other tools;
5) Be ineffective as companies would find ways to pay the ransoms;
6) Reduce reporting of ransomware incidents by Australian organisations, reducing the Government's visibility of the problem; and
7) Make companies covered by exceptions more likely to be targeted by malicious actors.

Finally, Government is unlikely to consistently enforce a law prohibiting ransom payments.

The reasoning for each of the above assertions is provided below.

1) Do little to reduce cyber crime in Australia

Although the number of ransomware attacks has increased drastically in recent years, it has remained relatively stable as a percentage of overall cyber crime.

For example, cyber security company Mandiant reported that ransomware investigations made up 23% of their incident response investigations in 2021, down from 25% in 2020[1].

In the remainder of attacks, malicious actors attempted to obtain Personally Identifiable Information (PII), Protected Health Information (PHI), Payment Card Industry (PCI) information, intellectual property, or other sensitive business or financial information from their victims. This information has value to cyber criminals because it can be sold to others (or used by the attackers themselves) for the purposes of carrying out fraud: using stolen credit card data to make fraudulent purchases, performing fraudulent financial transfers into criminal-controlled accounts, performing unauthorised cash withdrawals, taking out loans, opening lines of credit, or committing other types of crime under the victim's name.

[1] Mandiant, 2022. *M-Trends 2022 Mandiant Special Reports* [online] Mandiant. Available at: <https://www.mandiant.com/m-trends> [Accessed 15 April 2023].

If the Government prohibited the payment of ransoms and extortion demands, and assuming that such a ban was actually effective in preventing the victims of cyber crime from paying ransoms, malicious cyber actors would continue to target Australian organisations, simply shifting their tactics to those which ensured their ability to continue monetising their criminal activities.

2) Destroy many businesses that fall victim to cyber attacks which might otherwise be able to survive by paying a ransom

Significant IT outages, including those caused by cyber security incidents, pose an existential threat to many organisations. There are numerous public examples of businesses shutting down as a result of a ransomware attack.

A 2022 survey conducted by McGrathNicol found that 79% of Australian businesses that had experienced a ransomware attack chose to pay the ransom[2]. Although the McGrathNicol report does not provide an in-depth explanation for why such a high percentage of businesses chose to pay a ransom, the report does state that "*Businesses are over-confident in their abilities to respond to a ransomware attack, but the reality is that many are still very unprepared.*"

Cybereason's 2022 report *Ransomware: The True Cost to Business* provides insight into why businesses choose to pay ransoms. According to this report, "*Of the organizations that paid one or more ransom demands following successful attacks, nearly half (49%) said their primary motivation for paying was to avoid any loss of revenue, while 41% cited the need to expedite recovery as the main driver for payment ... 27% said they paid the ransom because they hadn't backed up their data. One-third (34%) indicated they were simply too short-staffed to attempt an effective response without the assistance of the attackers...*"[3]

Prohibiting the payment of ransoms would place enormous strain on those businesses that have not backed up their data, are too short-staffed to deal with the ransomware incident, or who are experiencing significant (and perhaps unsustainable) revenue losses due to the interruption posed to business operations resulting from a ransomware incident.

3) Cause significant harm to businesses who could recover operations only after a lengthy process

Prohibiting the payment of ransoms could cause significant disruption to businesses who can survive a ransomware outbreak, but where the loss incurred of revenue incurred as a result of an interruption to business operations far outweighs the cost of paying the ransom.

For example, in 2019 the U.S. city of Baltimore suffered a ransomware attack with the attackers demanding 13 bitcoin (approximately $80,000 USD at the time) in exchange for the decryption keys which could restore access to the city's network. The mayor at the time, Bernard C. Jack Young, decided to not pay the ransom, apparently after being advised not to pay by the U.S. Secret Service

[2] McGrathNicol, 2022. *Ransomware on the Rise* [online] McGrathNicol.
Available at: <https://www.mcgrathnicol.com/app/uploads/McGrathNicol_Flyer-Ransomware-on-the-rise_Final.pdf> [Accessed 15 April 2023]

[3] Cybereason, 2022. *Ransomware: The True Cost to Business* [online] Cybereason. Available at: <https://www.cybereason.com/hubfs/dam/collateral/reports/Ransomware-The-True-Cost-to-Business-2022.pdf> [Accessed 15 April 2023]

and FBI. As a result of this decision, the attack ended up costing Baltimore over $18 million USD when including the cost of remediation, new hardware, and lost or deferred revenue.

In this case, the decision not to pay demonstrated a lack of understanding of fundamental risk management principles, one of which is that the cost of a control cannot be justified if the cost is greater than the benefit realised. In other words, one must not spend $100 million to save $1 million. The City of Baltimore effectively spent $18 million USD to save $80,000 USD.

Another example of the significant ongoing harm that could be caused by a significant ransomware attack is the attack against Colonial Pipeline, a U.S. oil pipeline company in 2021. This attack resulted in Colonial Pipeline shutting down pipeline operations, leading to widespread fuel shortages in a number of U.S. states.

Although Colonial Pipeline was confident that they would have been able to eventually restore pipeline operations without paying a ransom, the enormous real-world impact of even a small interruption of their operations led to the company quickly deciding that paying the ransom was the best way to minimise the impact of this attack on Americans. Had Colonial Pipeline been prohibited from paying a ransom, fuel supply to U.S. East Coast would have been jeopardised. The CEO, Joseph Blount, said at the time "*I wasn't comfortable seeing money go out the door to people like this... but it was the right thing to do for the country.*"

4) Limit the options available to victims of cyber crime without providing them with any other tools

No one ever "wants" to pay a ransom. For executives, finding out that they have been compromised with a ransomware attack almost always comes as a complete shock. They have usually invested millions of dollars in cyber security and have trusted their defences, only to realise for the first time during a cyber attack that these defences were inadequate.

These same executives are invariably shocked that key systems have not been backed up, or that the backups don't work, or that the backups have also been encrypted. They are also shocked that they don't have a way of quickly resolving the incident without paying a ransom.

It is always with the utmost reluctance, disappointment and often embarrassment that executives agree to pay a ransom to criminals. These decisions are never made hastily or without exhausting every other conceivable option. When a decision to pay a ransom is reached, it is because executives cannot find a better way forward for the business, despite all their financial resources, technology, processes, internal and external expertise.

If the Government were to prohibit the payment of ransoms, it would remove a "last resort" option for a lot of businesses reeling from the impact of a devastating crime having been committed against them, without providing them with any assistance in return.

5) Be ineffective as companies would find ways to pay the ransoms

Prohibiting the payment of ransoms would be ineffective as organisations that have fallen victim to a ransomware attack which poses a significant threat to the business would find ways of indirectly meeting the attackers' demands.

Roger Grimes, Data-Driven Defense Evangelist at KnowBe4, correctly identified the key issues at play when he said "*If you outlaw ransom paying, you will immediately explode the amount of 'ransomware recovery' firms that claim they do not pay the ransom, but secretly do. There will be a whole lot of firms that claim AI or quantum computers or their own internal crypto experts allowed them to recover the encryption keys. You will have firms paying out of foreign-located entities. And you will have a lot more firms that simply do not get law enforcement involved, pay the ransom and never report it. You will be turning otherwise law abiding firms into unwanted criminals.*"

Companies that have no option but to pay a ransom in order to save their business will find creative ways to pay the ransom without running afoul of Australian law. This would likely result in the Australian Government having less visibility of ransomware attacks in Australia and having a lessor understanding of the extent of cyber crime in this country.

6) Reduce reporting of ransomware incidents by Australian organisations, reducing the Government's visibility of the problem

Prohibiting the payment of ransoms would reduce the likelihood of companies reporting ransomware attacks, since companies affected by a ransomware attack would investigate all their response options before committing to a particular course of action. In serious cases, where the existence of the company is at stake, this could include options which may be inconsistent with the law.

This would result in the Australian Government having less visibility of ransomware attacks in Australia and having a lessor understanding of the extent of cyber crime in this country. It may also result in a breakdown of relationships between the private sector and the Government, which could be viewed as increasingly out of touch with the realities of cyber crime and the difficult decisions that companies have to make to combat ever-evolving threats.

7) Make companies covered by exceptions more likely to be targeted by malicious actors

Government may be tempted to create exemptions to the prohibition on paying ransoms for organisations that are classified as "critical infrastructure", "networks of national significance" or some similar category. This may include electricity generation and distribution companies, water utilities or hospitals. However, if such organisations are exempted, it would put them at higher risk of attack in the event that such legislation is passed.

Allowing certain organisations to pay ransoms while prohibiting others from being able to do the same would effectively provide malicious actors with a list of organisations who are likely, under the right set of circumstances, to pay a ransom. Although this may result in an overall reduction of ransomware attacks against Australian organisations, those ransomware attacks that do occur are likely to be carried out against companies of national significance, have a much greater impact on ordinary Australians, and result in much higher ransoms.

Government is unlikely to consistently enforce a law prohibiting ransom payments

For those organisations that are not classified as "critical infrastructure", "networks of national significance" or some other category that Government may decide to exempt in legislation prohibiting the payment of ransoms, the willingness of Government to consistently prosecute those who pay ransoms in breach of the law is questionable.

While it may be easy to shape public opinion in favour of prohibiting ransom payments by propagating examples of high-profile cyber incidents affecting multinational corporations, the devastating reality of a ransom payment ban would become widely publicised soon after such a ban took effect.

When Australian businesses start collapsing because they were unable to continue operating without paying a ransom, those businesses owners and impacted employees will soon become the very real face of the cost of a ransom payment ban. The Australian public will then grasp the scale of the problem and public opinion could very well end up on the side of businesses simply attempting to stay afloat. Arguments in support of a ransom payment ban will likely not resonate with the general public once they see business collapsing and thousands of people losing their jobs directly as a result of the ban.

In such an environment, prosecuting businesses or individuals who choose to pay a ransom in order to save their business would be politically risky for any government. As such, the effectiveness of a ransom payment ban would be highly questionable.

g. Should Government clarify its position with respect to payment or nonpayment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

Government should help Australian organisations defend against cyber attacks by providing threat intelligence, hardening guides, and other resources to the Australian public in order to make Australian organisations harder targets for malicious cyber actors.

Once a cyber intrusion has occurred, however, the focus must shift to containing the incident and resuming business operations as quickly as possible, minimising the business impact of the incident. In some cases, paying a ransom may be the only way to resume business operations; in other cases, paying a ransom may be the faster and cheaper option by orders of magnitude.

The Government’s position should be that all decisions regarding payment or non-payment of ransoms should be risk-based and made after careful consideration of all the options, including whether it is possible to recover from the incident without paying the ransom (e.g. restoring systems from backups), the business impact of not paying a ransom (e.g. inability to continue as a going concern, billions of dollars in lost revenue), whether the actor has a history of honouring their commitments (e.g. providing decryption keys after a ransom payment has been made), whether the actor has a history of following through on their threats (e.g. to release sensitive customer information if a ransom is not paid), or whether the actor is a sanctioned entity.