KING&WOOD MALLESONS

Level 27
Collins Arch
447 Collins Street
Melbourne VIC 3000
Australia

T +61 3 9643 4000
F +61 3 9643 5999

www.kwm.com

TO Andrew Penn AO, Mel Hupfeld AO DSC,
Rachael Falk
2023-2030 Australian Cyber Security Strategy
Expert Advisory Board
auscyberstrategy@homeaffairs.gov.au

14 APRIL 2023

Dear Expert Advisory Board

King & Wood Mallesons' submission: 2023-2030 Australian Cyber Security Strategy discussion paper

We refer to your discussion paper for the development of the 2023-2030 Australian Cyber Security Strategy (**Strategy**) and thank you for the opportunity to make a submission on it.

1 What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

As the Board will be aware, many organisations rely on managed service providers (**MSPs**) and managed security service providers (**MSSPs**) to help administer their IT infrastructure and application support. While large organisations do so as well, the problem is particularly acute for smaller and medium sized organisations that may have no or limited IT staff that are responsible for managing their IT affairs. They often do not have the resources to have a full time CISO and often rely on MSPs or MSSPs to also manage their cyber security posture.

Organisations that do so are therefore particularly vulnerable if MSPs or MSSPs are compromised or if MSP/MSSP staff are themselves malicious actors. A common thread in many of the cyber incidents that we have advised on over the last 12 months is that the initial entry point into the organisation is a compromised MSP/MSSP personnel account. Given the role that MSPs/MSSPs play, these accounts are often privileged accounts that make it easier for malicious actors to compromise their targets.

In a recent case we assisted with, we reported the incident to the AFP who discovered that it was the contracted IT support worker of an MSP who had accessed our client's systems and illegally changed bank account details in its accounts payable system to his own benefit.[1] That person has now been charged for unauthorised access and modification with intent to commit a serious computer offence.

We therefore think that the Strategy should focus on ensuring that MSPs/MSSPs are as secure as possible given their importance in the IT ecosystem, and the unique advantages that targeting their personnel can confer upon malicious actors. This could be done in several ways, including by:

[1] https://www.afp.gov.au/news-media/media-releases/third-party-it-contractor-arrested-90000-fraud

- the introduction of an accreditation system for MSPs/MSSPs to provide assurance to customers that the MSPs/MSSPs have sufficient security measures in place to manage the security risks that they pose to their customers. This could include independent certification of compliance with appropriate standards, that is renewed at suitable intervals, or
- specifying MSPs/MSSPs as a data storage or processing service that falls within the data storage or processing sector under the *Security of Critical Infrastructure Act 2018 (Cth)* (**SOCI Act**). The *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules* could then be applied to MSPs/MSSPs so that they would be required to adopt an all hazards approach to their business, adopt a recognised cyber security standard and apply personnel checks to their staff who provide services to other entities. While this technically would only apply to MSPs/MSSPs who provide services to responsible entities for critical infrastructure assets, it would be preferable for them to be required to apply the same processes and standards to all of their customers.

  Changes would need to be made to the SOCI Act to address this and to specify MSPs/MSSPs as being responsible for a critical data storage or processing asset under the SOCI Act.

2 What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?

(a) What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?

We believe that reforms to improve cyber resilience through passing new legislation could be counterproductive. It can take significant time to consider, consult and implement legislation. This could result in organisations adopting a "wait and see" approach in updating their own cyber security practices. If industry participants are unsure of what their obligations will be due to prospective legislative change, they are more likely to wait for new legislation to come into effect, which leaves them vulnerable in the interim.

Further, without legislative harmonisation in the cyber security space, introducing reforms through new legislation could create greater confusion amongst individuals and organisations, particularly those who are already subject to multiple regulatory regimes that operate across different sectors. The required harmonisation is likely to also require an examination and amendment of existing regulatory regimes (eg the SOCI Act, the *Privacy Act 1988* (Cth) and sector specific regulation such as the APRA Prudential Standard CPS 234, *Telecommunications Act 1988* (Cth), the *Maritime Transport and Offshore Facilities Security Act 2003* (Cth) and the *Aviation Transport Security Act 2004* (Cth)) to remove overlap and duplication. It would also require a consideration of regulatory responsibilities and who would have regulatory responsibility for ensuring compliance with and enforcing any new cyber security legislation, and how that overlaps with regulatory powers currently vested in existing regulators.

We therefore think that regulatory reform should focus on ensuring consistency between the different regulatory regimes that currently regulate cyber security. Organisations should be able to have confidence that compliance with a single set of cyber security standards and processes will be sufficient to ensure compliance with all applicable regulatory requirements that apply to them. This will enable them to focus on ensuring their organisations are cyber secure rather than diverting resources and effort in managing a variety of regulatory requirements and regulators.

We also believe that any regulatory reform of legislation should continue to be principle based to give organisations flexibility to comply with regulatory requirements in a way that suits their circumstances. We also think that there should be greater use of guidance around cyber security to give organisations better insight into 'what good looks like'. The advantage of using guidance in this way is that it is flexible and can be implemented in a more efficient manner than legislation. At the same time, care needs to be taken to ensure that this flexibility is not exercised arbitrarily and without appropriate consultation and transition. Organisations which may have taken steps to comply with guidance at a point in time will need time to pivot if that guidance subsequently changes in a way which requires them to incur material costs or change their existing cyber security programs.

Finally, while we think that technical standards or regulations can be used as a means of improving cyber security resilience, this can be very prescriptive and should therefore be used with caution. While they are easier to pass and amend, as is the case with guidance, care should be taken around changes to the standards or regulations without appropriate time for transition.

(b) Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

We think that there is scope to amend the SOCI Act to include MSPs/MSSPs as set out in paragraph 1 above, or to clarify problematic definitions (particularly the definition of critical data storage or processing assets).

In relation to the specific question, we seek clarification of the policy reason behind the change. While the Minister for Home Affairs has criticised the existing SOCI, it is not clear to us what additional powers would be enlivened by the inclusion of customer data and systems within the definition of critical infrastructure assets. We believe that the powers given to Government under the SOCI Act are appropriate to protect Australia from catastrophic attacks on critical infrastructure.

We do not think that it is appropriate for those powers to be used for 'after the event' purposes to manage the fallout from a cyber breach, such as the disclosure of information to affected customers, or the establishment of compensation schemes. There are already existing legislative regimes or proposals to address these issues, including proposed changes to provide for private rights of action and statutory torts under the Attorney-General's Privacy Act Review Paper.

We also think Government should be cautious in interfering with an organisation's management of a cyber security incident unless specifically requested by the organisation. Doing so could mean that Government is responsible for how that incident is managed and dilute accountabilities that the organisation would otherwise have in relation to that incident.

(c) Should the obligations of company directors specifically address cyber security risks and consequences?

We do not believe that obligations of company directors should specifically address cyber security risks and consequences. Cyber security is merely a risk like any other risk assumed by organisations, and it is not clear to us that imposing this kind of duty on directors would make a significant improvement in the cyber security of Australia. While it would focus the minds of directors on compliance with those obligations, it is likely to simply result in more

documentation and processes around compliance, rather than a lift in cyber security resilience. Our clients often tell us that the time, effort and resources put into their cyber security programs are often distracted by focusing on compliance with audit requirements, rather than on improvements that actually make a significant difference to their organisation's cyber security resilience.

We do however consider that there is a very important role for guidance and education of directors around cyber security risks, which would provide them with the ability to ask the right questions and consider the right risks to mitigate. In this regard, we do commend the publication by the AICD and the Cyber Security CRC of their Cyber Security Governance Principles which is an excellent guide for directors.

(d) Should Australia consider a Cyber Security Act, and what should this include?

We think that passing new legislation will be counterproductive to the need to move quickly to enhance Australia's cyber resilience (see answer to question 2(a)).

(e) How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?

As set out in our answer to question 2(a), Government should seek to monitor and alleviate the regulatory burden on businesses through the simplification and harmonisation of regulatory frameworks.

An easy win would be to simplify the current process of notifying cyber security breaches to regulators so that organisations can notify one government entity of a data breach and know that this covers all other appropriate entities.

We do caution that this should not simply allow for information sharing between agencies without consent. Information should be shared between agencies that also have a regulatory function only for the purpose of simplifying the notification process. There must be measures in place to ensure that information given to one agency cannot be utilised for enforcement purposes by another regulator against the notifying party. Those other regulators should rely on their own existing regulatory powers to obtain any information they need for enforcement purposes.

(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?

As we stated in our opinion piece in the AFR, we believe that the payments of ransoms should be made unlawful.[2] Companies will thereby be afforded greater clarity when faced with a decision to pay a ransom or not. If the default position is that payment of ransoms and extortion demands are prohibited, the decision to not pay a ransom will be much easier for a board to make. However, we note that this could also have adverse consequences in certain circumstances.

For this reason, we believe that a safe-harbour exception should also be established if a company notifies the Australian Cyber Security Centre on a confidential basis that it intends to pay the ransom, and it believes, in good faith and on reasonable grounds, that paying the ransom is reasonably necessary to enable the company to continue to provide essential services, to lessen or prevent a serious threat to the life, health or safety of any individual, or to protect public health or safety. We also suggest that if an organisation does rely on the safe harbour exception to pay a ransom, that the safe harbour protects the organisation against contravening sanctions laws or the criminal provisions relating to instruments of crime and terrorism financing.

We do not agree that having a safe harbour necessarily makes some organisations more at risk than others, given the fact that ransom attacks are often indiscriminate and target all vulnerable organisations. An organisation that may suffer damage if sensitive information that it holds is stolen by a cyber criminal will inevitably find itself vulnerable to being attacked, whether or not it falls within a safe harbour for payment of ransoms.

Banning the payment of ransoms would disrupt the economics of the ransomware industry and is an important piece of the puzzle in attacking those who would seek to profit from this criminal activity. At present, the rewards that attackers can earn from a ransomware attack are extraordinary compared to the effort involved in mounting that attack.

If ransom payments are made unlawful (and even if they are not), it will be important for there to be clear and easily accessible support made available to victims of cyber-crime, for example:

- Operation Guardian should be extended to cover all known material cyber security incidents, so that customers whose information has been stolen have comfort that law enforcement is doing its best to protect their interests,
- it should be simple for them to replace identity documents and to understand when and where replacement is necessary and when it is not. This will also help organisations that have suffered a cyber security incident given the cost of replacing IDs can be very material where replacement is not necessary, and

[2] https://www.afr.com/technology/making-cyber-ransom-payments-unlawful-would-help-boards-20221120-p5bzp7

- they should be able to obtain clear advice as to how to protect themselves against identity theft and fraud. The support provided by IDCARE is excellent, and if required, they should be given more resources to undertake their important work.

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

See our answer to question 2(i) above.

8 During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?

Yes, the ACSC should be subject to an explicit obligation of confidentiality to allow for greater information sharing between themselves and companies experiencing a cyber incident. Organisations should be able to alert the ACSC without fear of other regulators gaining this information and using it for enforcement purposes.

9 Would expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?

We do not think that doing so would improve public understanding of these sorts of incidents. We do think that more education is required of all stakeholders, including those in Government, around the complexities of responding to and investigating a cyber incident. There is often a lack of understanding - for example, that it can, in some cases, take several months to analyse data that has been stolen to understand what information was in that data set and who it relates to.

Simply expanding the notification of cyber security incidents to include incidents which are not likely to cause serious harm to affected individuals would, in our view, be counterproductive. It would cause unnecessary concern (particularly among the less technology literate members of the community) or cause notification fatigue (which is problematic where there is a real risk of serious harm).

13 How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?

(a) Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

Yes, see our response to question 2(e).

KING&WOOD MALLESONS

15 ***How can government and industry work to improve cyber security best practice***

(a) ***What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?***

Small businesses need easily accessible and clear advice and assistance on how to best manage their cyber security. Government should invest in providing additional resources and guidance about what businesses should do and, if accreditation for MSPs/MSSPs is implemented as we suggest in our response to question 1, accreditation could be extended to cyber security consultants who would be able to assist small businesses to implement systems and procedures to manage their cyber security risks.

We would be happy to discuss if you have any questions in relation to our submissions.

Yours sincerely

[redacted]

Cheng Lim | Partner
King & Wood Mallesons

T [redacted]
M [redacted]
F [redacted]
E [redacted]
Partner profile