

1 March 2024

Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

To whom it may concern,

Cyber Security Legislative Reforms: consultation on proposed new cyber security legislation and on changes to the Security of Critical Infrastructure Act 2018

Sydney Airport acknowledges the Australian Government's stated commitment to shepherding a new era of genuine public-private co-leadership to enhance Australia's cyber security and resilience.

We welcome the opportunity to provide input as part of the consultation process into proposed legislative reform on new initiatives to address gaps in existing laws and amendments to the *Security of Critical Infrastructure Act 2018* to strengthen protections for critical infrastructure.

Please find below responses to select questions as listed in Attachment A of the Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation Paper.

Part 1 – New cyber security legislation

Measure 2: Further understanding cyber incidents – Ransomware reporting for businesses

8. What mandatory information, if any, should be reported if an entity has been subject to a ransomware or cyber extortion incident?

Considering the burden to gather and structure information falls on the entity at a critical time, flexibility to provide non-critical information at a later stage and enable efficient and timely reporting would be encouraged. Mandatory information for provision during the immediate period following an incident could include the details of the threat actor, the ransomware payment quantum and any communication.

9. What additional mandatory information should be reported if a payment is made?

If payment is made, then it would be reasonable to request payment details and facilitation mechanisms so that payment can be traced and potentially intercepted.

10. What is the appropriate scope of a ransomware reporting obligation to increase visibility of ransomware and cyber extortion threats, whilst minimising the regulatory burden on entities with less capacity to fulfil these obligations?

The small business cap is reasonable for mandatory reporting. However, non-mandatory reporting should be encouraged given a significant number of payments could be processed by smaller businesses.

12. What is an appropriate time period to require reports to be provided after an entity experiences a ransomware or cyber extortion attack, or after an entity makes a payment?

This is either for law enforcement, or for reporting and information gathering. The timeframes should be defined by the purpose. Asking for an overwhelming amount of information will restrict the timeframe reporting can be mandated in. The recommendation for information gathering would be to have the timeframe after all existing notification periods, which are targeted at law enforcement.

13. To what extent would the no-fault and no-liability principles provide more confidence for entities reporting a ransomware or cyber extortion incident?

To further victimise businesses and individuals already the victims of a ransomware attack would work against the national interest.

14. How can the Government ensure that no-fault and no-liability principles balance public expectations that businesses should take accountability for their cyber security?

There are already laws in place to protect the data of Australian individuals. These laws should be modernised to ensure they keep pace with the threats faced. We do not believe new laws that further criminalise already criminal behaviour will have any additional impact.

16. What types of anonymised information about ransomware incidents would be most helpful for industry to receive? How frequently should reporting information be shared, and with whom?

Payment values, data amounts, data types, and initial ransomware delivery mechanisms are all valuable to improve cyber security posture. This information could be shared quarterly to bi-annually.

Measure 3: Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator

17. What should be included in the ‘prescribed cyber security purposes’ for a limited use obligation on cyber incident information shared with ASD and the Cyber Coordinator?

We are of the view that while industry would like to be open and share information as required an organisation may prefer to keep some discussions private. Allowing for said discussions to be had privately will encourage freer flow of information and facilitate more effective collaboration.

18. What restrictions, if any, should apply to the use or sharing of cyber incident information provided to ASD or the Cyber Coordinator?

Information should be shared on a ‘need to know’ basis in order to facilitate open and honest collaboration. Detailed information can be shared more broadly after the initial threat has passed.

Measure 4: Learning lessons after cyber incidents – A Cyber Incident Review Board

20. What should be the purpose and scope of the proposed Cyber Incident Review Board (CIRB)?

The purpose and scope of the proposed CIRB should be to understand the root causes behind large scale cyber incidents in order to prevent harm to individuals in the longer term. This should also consider the impact any laws have had on cyber compliance, and how those laws could drive non-compliance. The scope should be generally limited to larger scale events, whether through volume of individual data breaches, severity of impact and the data leaked, as well as the likelihood for further harm or misuse, as some examples.

21. What limitations should be imposed on a CIRB to ensure that it does not interfere with law enforcement, national security, intelligence and regulatory activities?

The CIRB should be limited to information gathering only so that any enforcement activities are not impacted.

22. How should a CIRB ensure that it adopts a ‘no-fault’ approach when reviewing cyber incidents?

The ATSB model proposed is a reasonable way forward, a large-scale cyber event is not typically caused by a simple human failure, but a multitude of decisions taken in the lead up, many of which were likely to have been fair and reasonable.

24. Who should be a member of a CIRB? How should these members be appointed?

Senior independent members of high standing in the community, appointment must not be politicised and should be based on experience and merit.

25. What level of proven independent expertise should CIRB members bring to reviews? What domains of expertise would need to be represented on the board?

Members of the CIRB should be technical experts in the field of information technology and security. It would be most helpful for the Australian public to have a review board with suitably qualified staff, so as to truly understand why an incident may have occurred. The intention should be to avoid further victimising those members of businesses affected by cybercrime and to provide information and education to the broader business community where appropriate.

26. How should the Government manage issues of personnel security and conflicts of interest?

There should be no conflict of interests. Any conflicts must be declared and those members must recuse themselves.

27. Who should chair a CIRB?

The chair could be a senior member of the Australian public or judiciary. Similarly, to the model of a chair of an anti-crime commission.

29. What powers should a CIRB be given to effectively perform its functions?

Information should be able to be compelled, otherwise it would be easy to hide the truth from the CIRB.

30. To what extent should the CIRB be covered by a 'limited use obligation', similar to that proposed for ASD and the Cyber Coordinator?

The information produced for investigation should only be used for the purposes of a report into the incident. Further criminal charges should be the domain of law enforcement.

32. What design features are required to ensure that a CIRB remains impartial and maintains credibility when conducting reviews of cyber incidents?

The membership and purpose of the CIRB are key factors in ensuring impartial and credible conduct when reviewing cyber incidents.

33. What design features are required to ensure a CIRB can maintain the integrity of and protection over sensitive information?

Information must be stored in such a way as that the technology mega-corporations could not compromise it. Recent breaches of Microsoft have proven that these companies cannot protect information from motivated attackers.

Part 2 – Amendments to the SOCI Act

Measure 5: Protecting critical infrastructure – Data storage systems and business critical data

34. How are you currently managing risks to your corporate networks and systems holding business critical data?

Risk management of systems holding critical data is an ever-changing burden, with the balancing of security requirements over access. In a business setting, it may be possible for security requirements to take less precedence over day to day business operations, and this can mean that the controls protecting critical data are not as strong as necessary.

35. How can the proposed amendments to the SOCI Act address the risk to data storage systems held by critical infrastructure while balancing regulatory burden?

Third parties offering a service for data storage should be held to the highest standard, it is often impossible for a business to get a deep understanding of the security controls present in a third-party offering, so the government should take a very severe stance on any data breach in such a service.

36. What would be the financial and non-financial impacts of the proposed amendments? To what extent would the proposed obligations impact the ability to effectively use data for business purposes?

The definition of business critical data would need to be fairly well understood, it appears as if the intent is to classify many types of personal information as business critical, as well as some operational data, however this could result in these changes applying to every data storage location at an entity, which would greatly burden the entity and make compliance impossible. The operational use of some of this business-critical data should not be restricted too greatly, so that the systems which host items like encryption keys can be dispersed and protected at the level expected of their threats.

Measure 7: Simplifying how government and industry shares information in crisis situations – Protected information provisions

40. How can the current information sharing regime under the SOCI Act be improved?

The protected information sharing regime is extremely unclear in its current form. This makes continuing technical work difficult for entities, and very likely results in mass non-compliance. Protected information should be more strictly defined, and the cases for disclosure must be simplified. A similar model to how data processing works under the GDPR-EU could be adopted, where data processors must also comply with controls and have obligations. These obligations could be defined by the entity, in the form of contractual controls and would allow for a high-level engagement framework between an entity and another organisation where protected information could be shared.

41. How would a move towards a 'harm-based' threshold for information disclosure impact your decision-making? Would this change make it easier or more difficult to determine if information held by your asset should be disclosed?

Making the threshold harm-based would only further cloud the already murky cases for when information can be disclosed. The determination of harm is something still not settled in the data breach notification legislation, and the potential harm of protected critical information being disclosed would be significantly more difficult to assess. Simplifying the legislation around secrecy is a straightforward step to ensure compliance and should be prioritised.

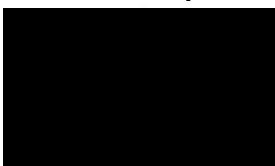
Measure 8: Enforcing critical infrastructure risk management obligations – Review and remedy powers

42. How would the proposed review and remedy power impact your approach to preventative risk?

It is reasonable that a deficient CIRMP is able to be remedied under the legislation.

I trust this information is of assistance to the Department of Home Affairs in its consideration of Cyber Security Legislative Reforms. Should you require further information please contact Joe Dennis, Head of Public Affairs ([REDACTED]).

Yours sincerely,



Karen Halbert
Chief Corporate Affairs Officer