Australian Information Industry Association

Submission on

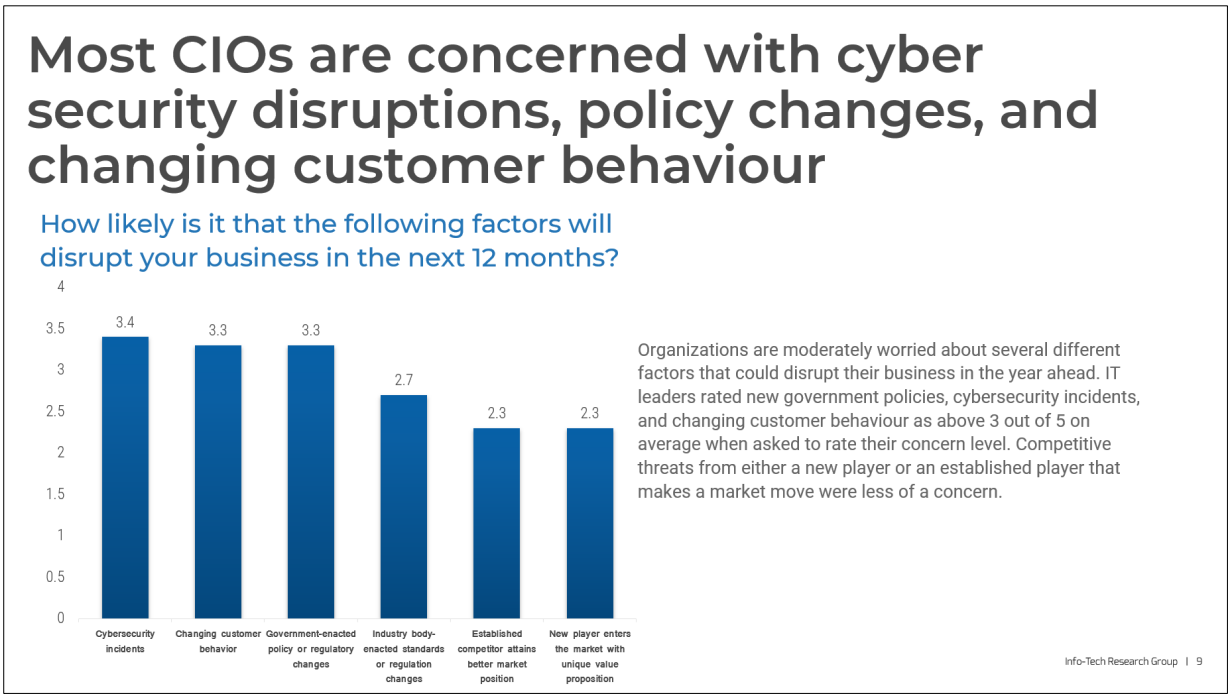
2023 - 2030
Australian Cyber Security Strategy:
Legislative Reforms

01 March 2024

Introduction

The Australian Information Industry Association (AIIA) thanks the Department of Home Affairs for the opportunity to respond to the consultation paper on the 2023-2030 Australian Cyber Security Strategy: Legislative Reforms.

The technology industry stands ready to support the Government and assist in uplifting cyber security to protect the national economy. According to the AIIA Tech Index, the technology sector is still implementing previous cyber security-related laws and investing heavily in cyber uplift. Notwithstanding, they are concerned about government continuing to introduce new regulations on a regular basis which is seen as disruptive to their business.



In principle, the AIIA supports information sharing and harmonising incident reporting. Secure platforms for voluntary threat intelligence sharing are essential. The AIIA supports industry collaboration, information sharing hubs, and incentives for sharing with law enforcement and government agencies. In addition, Streamlining existing incident reporting requirements would reduce administrative burdens. The government should clarify reporting obligations across frameworks to improve compliance.

For this reason, we are keen to ensure the request of data is necessary and proportionate, avoiding the divulging of commercially sensitive information. We are also motivated to ensure the cyber security regime is set up for success by ensuring ease of compliance and alignment with international standards.

Based on the abovementioned principles, the AIIA makes the following recommendations.

Part 1: New cyber security legislation

Measure 1: Secure-by-design standards for Internet of Things (IoT) devices

1. **Who in the smart device supply chain should be responsible for complying with a proposed mandatory cyber security standard?**

   Consistent with the *Product Security and Telecommunications Infrastructure Act* (*PSTI Act*) in the UK, the device manufacturer, distributor or importer (i.e. first entity in the supply chain and subject to Australian law) should be responsible for complying with a proposed mandatory cyber security standard. Roles in the value chain should be clearly delineated so that it is only the entities with the responsibility for, and knowledge of how a device is operating that are subject to notification requirements and standards. For IoT devices that use software and other component parts manufactured by third parties, the software and component part providers should not bear responsibility as they have no visibility as to the finished device, its overall functioning or the information that it is capturing.

2. **Are the first three principles of the ETSI EN 303 645 standard an appropriate minimum baseline for consumer-grade IoT devices sold in Australia?**

   The first three principles are appropriate given their adoption and incorporation into UK and EU legislation. These principles form the basis of the *PTSI Act* and are being taken into consideration as part of the EU *Cyber Resilience Act*. In respect of time for updates, a prescriptive approach should not be taken. Rather, a flexible approach based on industry best practice for the software in question should be adopted. Further, it should be made clear that responsibility for the application of updates should rest with the responsible entity (that is, the device manufacturer, distributor or importer).

3. **What alternative standard, if any, should the Government consider?**

   The AIIA suggests that the Government to follow the SOCI approach to recognise other "adequate standards". Whilst the list of countries aligned to ETSI is significant, it is possible other countries may choose ISO/IEC standards such as IEC2740 where there is overlap of principles.

4. **Should a broad definition, subject to exceptions, be used to define the smart devices that are subject to an Australian mandatory standard? Should this be the same as the definition in the PTSI Act in the UK?**

   Definitions should follow the *PTSI Act* and EU *Cyber Resilience Act* as closely as possible to ensure international consistency and prevent multiple disparate laws and regulations across the world. Given Australia is a comparatively small market on a global scale, having different or additional regulation to other major jurisdictions could reduce Australia's attractiveness as market for IoT devices and reduce the availability of important technologies in Australia.

5. **What types of smart devices should not be covered by a mandatory cyber security standard?**
The AIIA supports a clear description of 'smart devices' to ascertain regulatory scope and adds that Smartphones and laptops should be excluded.

6. **What is an appropriate timeframe for industry to adjust to new cyber security requirements for smart devices?**
In this circumstance a 12-month period may be insufficient, particularly as many devices are manufactured in foreign jurisdictions and Australia is a comparably small market. While the PTSI Act is coming into force in 2024, a 36-month transition period, aligned with the EU *Cyber Resilience Act*, would be more appropriate and facilitate greater compliance.

Measure 2: Ransomware Reporting for Businesses

8. **What mandatory information should be reported if an entity has been subject to a ransomware or cyber extortion incident?**
The AIIA seeks careful consideration and definition of a successful ransomware breach to increase understanding to avoid ambiguity and ensure consistent reporting from the outset.

- Ensure the new reporting regime focuses on demonstrably improving security by creating
  1) uniform and consistent reporting forms, supported by programmatic reporting capabilities and
  2) select reporting elements that would give the Government the ability to provide some reciprocal benefit to the impacted party or broader cyber ecosystem.
- Include reference to the digital security requirements for the collection, storage, and protection of reports submitted, which may itself be a valuable target for cyber adversaries.
- Harmonise with similar reporting regimes domestically and globally, recognising that shared cyber security goals are ultimately undermined if entity-level incident response procedures are unduly disruptive.
- Lower the annual turnover threshold for reporting entities to $AUD 3 million to capture a larger segment of the Australian economy to ensure the regime provides the Government with greater fidelity of the ransomware threat.
- Clearly limit cyber incident threshold to confirmed incidents where an entity makes a ransomware or extortion payment.
- Provide guidelines or procedures for third-party submitters, continuing to clarify that
  1) third-party firms are not required to submit reports on behalf of clients, but can do so when the client has expressly enlisted them to submit such a report, and
  2) that the ultimate responsibility to submit cyber incident reports rests with the regulated entity.
- Incorporate "no-fault" and "no-liability" principles into the ransomware reporting obligation to address a critical barrier to effective cyber security defence: the fear of reputational damage and legal repercussions.

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

The AIIA is concerned that there is no incentive to share the requested data if it can be used against them. Sharing of information should be by critical infrastructure entity impacted by cyber incident (in line with the shared responsibility model where service providers are contractually obligated to report to customers). This will help prevent double reporting and sharing of information. For these reasons, the AIIA suggests:

- Clearly define what is "cyber incident information" is, noting the AIIA proposed definition of "cyber threat indicators" should be as per cl 6 of the US CISA Act .
- Clearly define the purpose that disclosed information will be used for to enhance the certainty of how the limited use obligation will apply and provide further reassurance to affected entities that regulators cannot liberally interpret the limited use obligation to leverage the information provided to Australian Signals Directorate (ASD) and/or the Cyber Coordinator as part of an investigation or for compliance activities against them.
- Clearly define how to share information and what type of information should be shared. There should be clearly drawn boundary of information around types of information that can be on-shared.
- Given the sensitive nature of the information being shared, seek the entity permission before on-sharing disclosed information or at the very least alert them to the Government's intent to disclose.
- Given the sensitivity of the information, any agency entrusted with such sensitive information must have strong cyber security practices in place to protect such information from unauthorised access or disclosure.
- Exempt the disclosed information from Freedom of Information (FOI) laws.

Measure 4: Establishing a Cyber Incident Review Board (CIRB)

20. What should be the purpose and scope of the proposed CIRB?

The CIRB should focus on reviewing cyber incidents that have a "significant impact" on the availability of a critical infrastructure asset as defined under the *Security of Critical Infrastructure Act* 2018.[1]

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

The information obtained from the course of conducting a CIRB review should be subject to clear boundaries/protections and cannot be used for any investigation or compliance activities. The CIRB should not be provided with information gathering power to ensure the public perception remains positive, objective and independent.

[1] SOCI Act, Section 30BEA (Significant impact).

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

It is important that the CIRB has representation from a full range of industries and sectors, so that specialist industry knowledge can be applied to reviews and recommendations. Equally, input from members with a variety of industry perspectives will promote cross-industry information sharing and may generate new and innovative solutions. The UK has recognised the benefits of specialist industry knowledge in reviewing cyber incidents in the industry boards it has established to assist in that process. For this reason, the AIIA suggests:

- Prioritise industry membership of the CIRB based on incident response expertise to ensure that the CIRB can effectively carry out its functions.
- Ensure the independence of the board and provide clear mechanisms for appointments and decision making.

28. Who should be responsible for initiating reviews to be undertaken by a CIRB?

A CIRB review should be initiated by the CIRB itself, with majority agreement, *not* solely at the discretion of Government representatives.

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

The AIIA also recommends that the CIRB to have dedicated resources to enable the timely production of incident response reports that are both relevant and impactful. Its findings should be made public to enable a wider range of stakeholders to benefit from the insights gained from the CIRB's reviews, thereby strengthening the cyber security ecosystem as a whole. Furthermore, CIRB recommendations should be subject to metrics to analyse whether they are impactful.

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

CIRB should appropriately protect sensitive business information shared during its investigations - including making it exempt from Freedom of Information Act (FOI) requests.

Part 2: Amendments to the *Security of Critical Infrastructure Act* 2018 (*SOCI Act*)

Measure 5: Data Storage Systems and Business Critical Data

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?

The AIIA understands the need to plug the gap by ensuring that both business-critical datasets stored in the cloud (data storage and processing sector) and on premises should be subject to the same *SOCI* obligations/ Risk Management Program. For this purpose, only, the AIIA supports expanding the definition of "asset".

Otherwise, the broad expansion of the definition of "asset" to include "data storage systems" holding "business critical data" where vulnerabilities in these systems "could" have a "relevant impact" on critical infrastructure has the potential to significantly broaden the scope of entities considered a "responsible entity" for a "critical infrastructure asset." The threshold of "could" and "relevant impact" is too low. A higher threshold of "likely" and "material impact" would see a more targeted application of *SOCI Act*, and help see that third party entities (not subject to SOCI otherwise than by virtue of providing a "data processing or storage service") are not

subject to extensive regulatory burden where data is held in their system, but the entity operating in the critical infrastructure industry has other copies of the data elsewhere, or the data is encrypted and unable to be read by another party, even if unauthorised access occurred.

Measure 6: Consequence Management Powers

The AIIA opposes the extension of Part 3A step in powers, which should be reserved for national emergencies only. We note that there is a further need to identify the thresholds (i.e. harms-based approach) before these step-in powers are exercised. In terms of powers, we also note that having an "authorise" power of last resort is less contentious than the proposed directive and authorising powers. As for safeguards, there should be an appeal mechanism for organisations to rely on if in the event they are not able to comply with the direction due to nature of its business.
Further, the AIIA recommends:

- Restrict what directions the Government can issue to reduce unintended consequences.
- Reduce the application of the proposed power so that there needs to be more than a "causal link", and that the proposed power cannot be exercised when the consequence of an event "is imminent".
- Raise and clearly define the thresholds to use the power as it is reasonably foreseeable that an entity could be deemed "unwilling or unable" should they disagree with the Government as to the best course of action in response to a cyber security incident.
- Clarify Ministerial safeguards for the 'data processing and storage' sector.
- Given the breadth and uniqueness of the proposed power, legislate an appeal and review right via the *Administrative Decisions (Judicial Review) Act* 1977 (*ADJR Act*).
- Consider the potential International precedent this power creates and how it could enable other countries to make the same arguments with respect to technology companies operating at the direction of their Government.

Measure 7: Simplifying Protected Information Provisions

- Given the breadth and subjective nature of the thresholds, restrict the purposes for which a disclosure of "protected information" can be made and clearly define the thresholds for disclosure.
- Consult and advise the relevant organisation/s that the Government intends to share their protected information and inform them as to the intended recipient and rationale.
- Given the sensitivity of the information collected under the Act, we also recommend that the Government impose an obligation to keep information safe and secure.
- Any party whose information has been shared should be afforded a legislated appeal right under the *ADJR Act* should they disagree with the decision of the Government.
- Change the term "Protected Information" in the *SOCI Act* to "Restricted Information" to avoid further confusion between the "Protected Information" in the *SOCI Act* and the "Protected" security classification in the Protective Security Policy Framework (PSPF).

Measure 8: Review and Remedy Powers

While we understand that there will be situations where a Critical Infrastructure Risk Management Plan (CIRMP) is so "seriously deficient" that it requires the Government to step in, we note that not all CIRMP-related obligations have entered into force and would encourage the Government to refrain from introducing this power until it is fully in force.

Measure 9: Telecommunications sector security under the *SOCI Act*

The AIIA is concerned with the process the Attorney-General will undertake to make a technical assessment when there is a need to over-ride the Privacy Act and would like Attorney-General to consult with affected entity first to agreeing to do so. We are also keen to understand if there will be internal/external reviews of government requests for data or inform the consumer if industry suspects an overreach.

Conclusion

The AIIA appreciates the opportunity to make a submission. Should you have any questions, please contact Ms Siew Lee Seow, General Manager, Policy and Media at siewlee@aiia.com.au.

Yours sincerely
Simon Bush
CEO, AIIA

About the AIIA

The Australian Information Industry Association (AIIA) is Australia's peak representative body and advocacy group for those in the digital ecosystem. We are a not-for-profit organisation to benefit members, which represents around 90% of the over 1 million employed in the technology sector in Australia. Since 1978, the AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment for our members and to contribute to Australia's economic prosperity.

We do this by delivering outstanding member value by:

- providing a strong voice of influence
- building a sense of community through events and education
- enabling a network for collaboration and inspiration; and
- developing compelling content and relevant and interesting information.

We are unique in that we represent the diversity of the technology ecosystem from small and medium businesses, start-ups, universities, and digital incubators through to large Australian companies, multinational software and hardware companies, data centres, telecommunications companies and technology consulting companies.