March 1st 2024

Hamish Hansford
Deputy Secretary of Cyber and Infrastructure Security Group
Department of Home Affairs

Electronic via Consultation Web Form

Dear Mr Hansford,

Cyber Security Legislative Reforms Consultation Paper

The CISO Tribe welcomes the opportunity to provide feedback on the *2023 - 2030 Australian Cyber Security Strategy Legislative Reforms* Consultation Paper.

The CISO Tribe (150+ members) in Australia stands as a dynamic and inclusive peer-to-peer community, purposefully designed for CISOs to engage in thought leadership.

The membership criteria is such that the majority in the group holds the CISO title, if not, they would be the most senior executive that is responsible for the cybersecurity strategy and responsibilities at their organisation. Our members are from some of Australia's top companies covering financial services, manufacturing, critical infrastructure, telecommunications, retail, legal, governments, and many more.

The CISO Tribe is a group that has organically expanded over the years since 2019 and continues to be driven entirely by diverse industry leaders. It remains community centered and focused on the CISOs' needs, while fostering an environment of collective growth and insight sharing.

The CISO Tribe LinkedIn page: https://www.linkedin.com/company/89489134

Measure 1: Helping prevent cyber incidents - Secure-by-design standards for Internet of Things devices

Responsibility to comply with a proposed mandatory cyber security standard

The CISO Tribe supports the adoption of secure by design standards for the Internet of Things (IoT) devices. Although a voluntary approach is already in place, based on the risk associated with IoT (consumer-grade) devices a mandatory cyber security standard will help increase the levels of adoption across industry.

Ensuring security in the smart devices requires collaboration and accountability among several stakeholders. Consensus of the CISO Tribe leans towards **manufacturers** bearing primary responsibility for ensuring that smart devices meet mandatory cyber security standards. This view parallels the car manufacturing analogy, where the responsibility for safety and compliance begins at the start of the supply chain. The idea of having a "gatecheck" at the point of manufacturing or importing, emphasises a critical control point where devices must be certified as compliant before being allowed into the market. However,

supplier and **IoT integrators** should also be responsible for complying with a proposed mandatory cyber security standards to ensure security standards are maintained through the device's lifecycle.

Furthermore, at a national level, the regulatory framework should oversee and control the entry of smart devices into Australia, allowing operation of only those that are compliant with the set of agreed standards.

Appropriateness of the standard to address current challenges

Adoption of an international standard like ETSI EN 303 645 is a positive step towards bringing Australia in line with our international partners. ETSI EN 303 645 provides a set of specific guidelines designed to secure IoT devices, making it a suitable candidate for establishing a minimum security baseline. Its focus on consumer-grade IoT devices addresses the unique challenges and threats faced by these devices directly. However, as IoT devices become integral to broader Operational Technology (OT) systems, the security of these devices impacts the security of the entire system. Therefore, applying security by design principles from IEC 62443 (which focuses on Security for Industrial Automation and Control Systems) to IoT devices could enhance the overall security posture of integrated systems.

The first three principles of the ETSI EN 303 645 standard are good starting points. In addition to the first principle aimed at eradicating universal default passwords in smart devices, careful consideration could be given to the incorporation of multifactor authentication (MFA) and/or more secure passwordless authentication methods such as passkeys.

Timeframe for industry to adjust to new requirements

For everyday consumer devices such as washing machines, kettles, and fridges, the CISO Tribe advocates for a "common sense" approach. This implies ensuring these devices meet minimum security standards without overly burdensome requirements, recognising their varied impact on consumer safety and privacy.

A risk-based approach is required to determine compliance timelines. This means that the timeframe for adjustment should be aligned with the level of risk associated with the device's potential cyber security vulnerabilities.

Engaging in dialogue with suppliers is seen as crucial to determining realistic and practical timelines. This engagement would involve assessing the suppliers' capacity to meet new requirements, their current cybersecurity practices, and any challenges they might face in adjusting to the new standards.

Smart devices which have the potential if compromised to cause significant harm to people, material assets, critical infrastructure, the environment or industry should be covered by an alternate standard or standards with higher security watermarks.

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

Information requested as part of ransomware reporting obligation

The CISO Tribe agrees that limited visibility of ransomware incidents and cyber extortion threat restricts the capacity of the government and private sector to effectively mitigate the impact of ransomware threat on society, the economy and individual well-being. A ransomware reporting obligation for businesses will help increase such visibility, but harmonisation and standardisation are essential. There's a clear call from industry for harmonised reporting obligations to simplify compliance and ensure consistency across different regulatory frameworks. This approach would benefit regulated entities like those who are in scope of several regulatory obligations (e.g. APRA, OAIC, SOCI, etc..), making it easier for them to meet reporting requirements without navigating a patchwork of regulations.

Basic information that is already requested by current regulators when an incident is reported should be considered as part of the ransomware reporting obligation.

In addition, threat information sharing helps enhance collective cyber security resilience. This includes sharing Indicators of Compromise (IoC) and understanding of threat vectors to enable timely and effective responses across the industry. Nevertheless, it is important to balance the need for sharing crucial threat information with the desire to maintain confidentiality, especially concerning legal and reputational risks. This balance is vital for encouraging entities to report incidents without fear of negative consequences.

Scope of ransomware reporting obligation

Reporting obligations across jurisdictions highlights the complexity of managing cyber incidents in a global context. This raises questions about the relevance and efficiency of reporting incidents to authorities in jurisdictions not directly impacted by an incident. Therefore, focus should primarily be directed towards incidents that directly affect organisations operating within Australia or that impact Australian customers. For instance, ransomware incidents affecting organisations with a global footprint, yet lacking any discernible impact on their Australian operations or customers, may be considered exempt from such reporting obligations.

On the other hand, the ransomware reporting obligation should encompass the majority of organisations across Australia to align with the overarching objectives of the Government, which include addressing limited visibility of the ransomware and cyber extortion threat. The obligation should not be confined solely to larger businesses with an annual turnover of $10 million. According to the Australian Small Business and Family Enterprise Ombudsman (ASBFEO), the vast majority of businesses in Australia are considered small businesses. These small businesses often serve as third-party suppliers to larger entities, including governmental bodies. Recent instances of data breaches underscore the reality that malicious actors frequently target small businesses to procure sensitive information, subsequently leveraging it for identity theft, credential stuffing attacks, and fraudulent activities.

Small to medium-sized organisations contribute valuable data to aid the Government and industry in comprehending the breadth and gravity of the ransomware threat landscape,

thereby facilitating the development of more efficient response strategies. Furthermore, by extending the regulatory obligation to encompass a majority of businesses, rather than solely focusing on large enterprises, the Government can provide resources, guidance, and assistance to affected buisnesses lacking robust cybersecurity capabilities, thus bolstering their ability to defend against and recover from ransomware attacks.

Recognising the varying capabilities of organisations, especially small to medium businesses, we suggest:

(a) Alignment with Privacy Act 1988 to cover businesses with an annual turnover of more than $3 million.
(b) A reasonable period of transition for small businesses, where voluntary reporting is recommended until broader awareness has been achieved.
(c) A tiered approach for mandatory information requested as part of the reporting obligations. This approach would tailor the reporting requirements to the entity's size, capacity, and the potential impact of the incident, thereby reducing the burden on smaller organisations while still ensuring valuable information is shared.

'No-fault' and 'no-liability' protection principles

Proposing a no-fault and no-liability reporting mechanism is consistent with the overarching objective of promoting timely and transparent reporting of ransomware incidents. By alleviating concerns regarding culpability (fear of blame) or exposure, organisations may be more inclined to promptly report incidents, thereby facilitating faster response and mitigation efforts across the affected sectors.

Regarding the enforcement mechanism for the ransomware reporting obligation, considering that incident reporting obligations are already established and enforced by regulatory bodies, it would be prudent to explore the adoption of similar enforcement mechanisms as those employed by current regulators, such as APRA and OAIC.

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

The CISO Tribe welcomes initiatives to encourage industry engagement with Government, including a limited use obligation for Australian Signal Directorates (ASD) and the Cyber Coordinator. We acknowledge the benefit of including 'prescribed cyber security purposes' such as:

- to assist the entity with preventing, responding to and mitigating the cyber security incident;
- to identify further potential cyber security vulnerabilities and take steps to prevent further incidents;
- to analyse and report trends across the cyber threat landscape, including the provision of anonymised cyber threat intelligence to government, industry and international cyber partners;
- to provide stewardship and advice to industry, including provision of advice to industry on cyber maturity and best practice risk mitigation across sectors; and

- to improve existing incident response mechanisms, such as incident reporting processes and coordination between government and industry.

Establishing clear definitions and specifications for each proposed 'prescribed cyber security purposes' will offer industry greater confidence regarding the utilisation of their information. For example, it would be beneficial to clarify the purpose "to facilitate **consequence management** after a cyber incident" and whether this is similar to the consequence management powers outlined in measure 6 of the consultation paper.

Moreover, as one of the 'prescribed cyber security purposes' is to share information provided with other agencies, the Government should consider requesting consent from the organisation impacted before sharing with other agencies, especially when those agencies are outside Australia.

In order to promote and incentivise entities to share information and collaborate with ASD and the Cyber Coordinator in the aftermath of a cyber incident, the Government could consider:

- Providing financial incentives, such as tax breaks, grants, or subsidies, for companies that actively engage in information sharing and collaboration.This can help offset the costs associated with cybersecurity improvements and incident reporting.
- Cyber incident government assistance and support should be offered to entities who lack capability in dealing with sophisticated cyber threats. This can include access to tools, expertise, and advice on mitigating threats and handling incidents.
- Offer liability protection for entities that share information about cyber threats and incidents. This can encourage more organisations to come forward as the fear of legal repercussions or damage to reputation often discourages/ prevents them from doing so.
- Provide credits to businesses who report on time. These credits can be used towards various government services.

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

The CISO Tribe considers the nation (Government, Industry and Individuals) will benefit from a Cyber Incident Review Board (CIRB) similar to the existing US Cybersecurity Review board (CSRB), where lessons learnt and best practices are shared with the public. In addition, the CIRB should prioritise major incidents with the potential for significant impact on Australia, aligning with the threshold established by the CSRB in the United States.

It is recommended that information is structured in a manner that prevents the release of information from causing commercial or reputational harm to impacted organisation(s).

While the CIRB should be able to request entities to provide information, powers should be restricted in cases where entities retain the right to control access to certain information, such as documents protected by legal professional privilege.

For the purpose of upholding impartiality and credibility, the preferred approach involves a combination of a core set of standing members across Government, industry and academia along with a pool of individuals who could be appointed to conduct specific reviews.

Finally, given the diverse CIRB membership composition, clear obligations should be outlined regarding how the CIRB must safeguard and handle sensitive and personal information. This includes protocols for anonymising and redacting data, as well as requiring affirmative confirmation from affected parties before sharing information with other government bodies, regulators, or external parties.

Thank you for the opportunity to provide our views on the Cyber Security Legislative Reforms. If you wish to discuss any aspect of this submission further, we would be happy to meet with the departmental staff. Please contact Shamane Tan and the steering committee at [redacted].

Kind regards,

Shamane Tan

CISO Community Tribe Founder and Representative