Australian Chamber of Commerce and Industry

Australian Cyber Security Strategy: Legislative Reforms

Submission to the Department of Home Affairs
March 2024

Introduction

ACCI welcomes the opportunity to provide feedback on the *Australian Cyber Security Strategy: Legislative Reforms Consultation Paper (Consultation Paper)*.

We support the government's efforts to strengthen the nation's cyber security posture and emphasise that a collaborative approach between government, industry, and the community is essential to achieving this goal.

This submission offers responses to relevant questions in the Consultation Paper. Our responses were formed following consultation with ACCI members, and in particular, the members of our Data, Digital and Cyber Security Forum.

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

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

The proposed mandatory cyber security standard should only apply to manufacturers and designers of products, as they are in the best position to make the technical changes required to comply with the proposed baseline measures.

Manufacturing should include the full supply chain for the manufacturing process, including all component / third-party parts.

From a software design/development perspective it would be worth further exploring how best to address the use of "Open Source" technologies that are so readily available. Mandatory measures could inhibit development of new technologies or drive up the cost of products.

Whilst it is customary to identify open-source technology within the products that use it, there are many notable examples where this has not happened.

Manufacturers should be required to certify their products to the proposed standard and provide visibility on the full manufacturing process as relevant to ensure openness and accuracy.

Importers, distributors, suppliers and others in the supply chain who cannot influence the design elements of products should not be captured. However, should importers, distributors and suppliers be deemed in scope in any way, they should not be required to make a determination about non-compliance with relevant security requirements. It is proportionate for their obligations to be limited to ensuring in-scope products are accompanied with a statement of compliance, and to report to the relevant authority if they are informed of non-compliant devices.

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

ACCI members agree that adopting the first three provisions of ETSI EN 303 645 would be an appropriate minimum baseline and align with the approach taken under the PSTI Act in the UK.

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?

The broad definition and types of devices captured under the UK legislation are supported. We encourage consistency with the PTSI Act where possible and appropriate.

What types of smart devices should not be covered by a mandatory cyber security standard?

Note again support for consistency with the UK legislation in regard to excluded products: charge points for electric vehicles, smart meters, medical devices and computers.

Our automotive sector members queried whether IOT in vehicles would be excluded or not.

What is an appropriate timeframe for industry to adjust to new cyber security requirements for smart devices?

Members noted that due to the nature of the requirements a two-year transition period would be more appropriate, particularly for manufacturers and designers. This is due to the changes not only impacting systems and reporting, but actual product design and manufacture. Within these businesses this would require identification of the changed requirements, changes to strategic planning and product pipelines, budget reviews etc.

If others in the supply chain are captured in the final scope, then the transition period should be staggered so that compliance commences for manufacturers (at least 6 months prior) ahead of importers and distributors. Should compliance commence at the same time for all parties, manufacturers could be compliant, but importers/distributors could be non-compliant as the devices they may have in stock could have been manufactured prior to the obligations commencing.

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

The Consultation Paper notes that the objective for mandating reports of ransomware incidents and payments is to assist the government with increasing visibility of the threat landscape to increase the capacity of the government and the private sector to help Australian organisations prepare for, and respond to, these incidents.

When considering a problem, government guidelines require the consideration of a range of policy options, including both regulatory and non-regulatory approaches.

We would argue that there is a less burdensome way to collect the desired information such as through a combination of approaches including: minor amendments to existing *Security of Critical Infrastructure Act 2018* (SOCI) entity incident reporting, increasing government entity incident reporting, information collected by the proposed Cyber Incident Review Board and other existing information exchange processes like the Trusted Information Sharing Network (TISN) and business surveys.

Amending existing incident reporting requirements (or improving report rates) for high value targets and high-risk entities such as government and critical infrastructure networks should be actioned first prior to imposing further regulatory burden on private entities, including small and medium businesses.

The *Commonwealth Cyber Security Posture in 2023*[1] report found that the percentage of (Australian Government) entities reporting cyber security incidents to ASD declined over the 2022-23 financial year from 51 per cent of entities in 2022, to 42 per cent of entities who indicated that they report at least half of the cyber security incidents observed on their networks to ASD.

There is also a question of ASD's capacity to respond to any significant increase in reports and the deterrent effect this could have on engagement with ASD if they are not seen as responsive and helpful. For example, the *Cybercrime in Australia 2023* report[2] noted that the outcomes from businesses reporting malware incidents voluntarily to police or ReportCyber varied from not

[1] Commonwealth of Australia 2023, Australian Signals Directorate, The Commonwealth Cyber Security posture in 2023, Report to Parliament November 2023

[2] Voce I & Morgan A 2023. Cybercrime in Australia 2023. Statistical Report no. 43. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sr77031

hearing anything (24.3 per cent), told nothing could be done (22.2 per cent) to being told their complaint would be investigated but nothing else (24.7 per cent).

Lastly, we would note that small businesses already make up the majority of ransomware reports[3] and government could partner with industry associations to convey the benefits of voluntary reporting in an effort to increase voluntary small business reporting further. Government could also look to partner with accounting software providers (or other small business tech infrastructure providers) to deliver a fit-for-purpose reporting mechanism for small businesses, rather than small businesses attempting to navigate the current reporting options.

Which entities should be subject to the mandatory ransomware reporting obligation? Should the scope of the ransomware reporting obligation be limited to larger businesses, such as those with an annual turnover of more than $10 million per year?

ACCI members supported mandatory reporting for SOCI covered entities through minor amendments to existing reporting obligations and the addition of ransom payment reporting.

Consideration could be given for a phased approach whereby Phase 1 captures amending reporting obligations for SOCI entities. This could be done in conjunction with encouraging all other businesses to voluntarily report and boosting ASD internal capacity to respond to voluntary notifications to demonstrate the mutual benefit to industry in reporting. Phase 2 would consist of a review of the effectiveness of phase 1 reporting changes and consideration of expanding the scope to other large and medium businesses with a carve out of small businesses if there remained an absence of data to build a cohesive threat picture.

ACCI's preferred definition of a small business, if a carve-out is supported overall, is that used by the ABS – *fewer than 20 employees*, rather than the ATO definition used in the paper.

Members reiterated that many of their small business employers have no/low computer literacy and would be unlikely to report the information desired by the agency and in a speedy manner.

Some ACCI members did note concerns about small businesses operating within critical infrastructure supply chains, the potential vulnerabilities in the chain they create and the benefit of visibility of the risk. It was unclear if they would be consistently captured by SOCI incident requirements and if not, how we might capture them as a distinct group of businesses. Further consultation may be appropriate to consider if capturing this group of businesses is appropriate, how best to capture them and the mechanism for this.

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

If it were only SOCI entities reporting as per our position above, then we believe the following data points (in addition to existing incident report requirements) would be sufficient:

- nature of malware attack (ransomware variant used and first point of entry if known),
- digital snapshot of the data and assets affected,

[3] Commonwealth of Australia 2023, Australian Signals Directorate, 2022–23 ASD Cyber Threat Report

- when and how a ransom request was made; and
- an option to upload further additional information (quantum of payment demanded, method of payment etc)

To increase the likelihood of reporting and to reduce the burden on businesses, the initial notification should be minimal as ASD can collate additional information as needed during follow up activity.

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

For the second reporting element this should be limited to: payment method (for example, the type of cryptocurrency used), the amount paid and to 'whom' money was paid.

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?

Noting our position that it should only be applicable to SOCI covered entities in the first instance, the reporting obligation should be consistent at 72 hours.

If the mandatory reporting obligation was to extend to other large and medium businesses, then a minimum 10-day reporting period would be more appropriate to balance urgency with complacency.

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

'No-fault' 'no liability' principles should apply for ransomware reporting if the goal is to increase reporting and threat visibility and the government has determined not to prohibit payments. If this changes then the principles should be reviewed.

Making voluntary reports anonymous or providing unique identifiers for reports would increase confidence further.

What is an appropriate enforcement mechanism for a ransomware reporting obligation?

An appropriate enforcement mechanism for this obligation would be civil penalty provisions as outlined in the Consultation Paper.

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

Timely and brief reports provided to impacted sector peaks would be useful for dissemination through existing networks along with public quarterly reports which also monitor trends over time.

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

What restrictions, if any, should apply to the sharing of cyber incident information?

Members main concern with the proposed obligation is that once a business engages ASD for assistance after an incident, ASD can share this information with other regulators under the 'limited use' terms. Although these regulators can't use this information to directly prosecute or for other compliance activities, the fact that they are aware company 'x' has had a cyber incident can create a red flag for them to then utilise their own powers to inspect the company e.g., if a regulator knows that business x was involved in an incident then they can go on the hunt for 'non-compliance'.

ASD should not be allowed to share information with regulators that enables them to identify the specific business, only anonymised or aggregate data. This is particularly the case if government wishes to encourage an increase in voluntary reporting and requests for assistance.

Industry would also want confirmation that this information would be protected from Freedom of Information requests.

What else can government do to promote and incentivise entities to share information and collaborate with ASD and the Cyber Coordinator in the aftermath of a cyber incident?

If government wants to incentivise entities to share information, then they must ensure the benefits to businesses outweigh the risks and they are provided with genuine assistance to respond and recovery from an incident (regardless of size and significance threshold).

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

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

ACCI supports establishing an independent Cyber Incident Review Board (CIRB).

We support the proposed purpose and scope of a CIRB but add that the CIRB should also review several small and medium business incidents each year. If the focus is only on significant incidents or incidents of severe consequences than SMEs would most likely never be captured.

It is critical that this body also analyses threats to our small business sector and produces information and lessons learnt if we want to uplift these businesses cyber maturity.

Participation by SMEs would be voluntary and there could be a mechanism established to notify the board of an incident for potential review or an information sharing mechanism established between ReportCyber and the CIRB. CIRB could look for trends in small business incidents and reach out to impacted businesses to enquire if they would participate in an investigation.

Who should be a member of a CIRB? How should these members be appointed? What level of proven independent expertise should CIRB members bring to reviews? What domains of expertise would need to be represented on the board? What design features are required to ensure that a CIRB remains impartial and maintains credibility when conducting reviews of cyber incidents?

The CIRB could consist of a set of standing members (as per option 1) plus a pool of individuals who could be appointed to facilitate a specific review depending on the impacted entity, the nature of the cyber incident and the type of vulnerability being reviewed.

This pool of individuals should consist of experts with small business backgrounds (i.e., lived experience of small business ownership), industry representation, cyber security expertise, and individuals experienced in risk and recovery.

The National Cyber Security Coordinator should Chair with a Department representative as an ex-officio position.

Members also noted that the appointments should be for two-year terms (even standing CIRB members) to ensure that policy agendas are not formed through the CIRB process. The terms could be overlapping terms, so that half of the standing members are rotated each year.

Those members (limited) who were familiar with the US model noted their support for the adoption of something as close as possible to this model.

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

ACCI supports CIRB reviews being initiated by the Minister for Cyber Security, the National Cyber Security Coordinator, the Cyber Incident Review Board or business self-nomination.

We do not support reviews being initiated by agreement between the Minister for Cyber Security and relevant Ministers.

What powers should a CIRB be given to effectively perform its functions? To what extent should the CIRB be covered by a 'limited use obligation', similar to that proposed for ASD and the Cyber Coordinator?

In the first instance, given we understand that the purpose of the CIRB is to act as an independent body that will invest the appropriate time and resources to examining the root cause of incidents and responses, we believe voluntary powers to request information but no powers to compel entities to participate in reviews should be sufficient.

Providing powers to compel entities and the use of these powers would be an additional burden on entities who may not wish to engage in what could be a lengthy investigative process after they have already been subject to significant business disruption and negative experiences (such as media scrutiny).

We thank you for your consideration of our feedback. Should you require any additional information or clarification of any points contained within, please contact Jennifer Low, Director Health, Safety, Resilience and Digital Policy at [redacted]