Tech Council

25 Aug 2021

Tech Policy Division
Department of Home Affairs
techpolicy@homeaffairs.gov.au

Thank you for the opportunity to respond to the consultation on strengthening Australia's cyber security regulations and incentives. As an organisation invested in the development and growth of Australia's digital economy, we see this dialogue as mission critical and welcome the consultation with industry on how to most effectively develop approaches to cyber security.

About the Tech Council of Australia (TCA)

The TCA is Australia's peak industry body for the tech sector. The Australian tech sector is a pillar of the Australian economy, contributing $167 billion per annum to the Australian economy, and employing 861,000 people. This makes the tech sector equivalent to Australia's third largest industry, behind mining and banking, and Australia's seventh largest employing sector.

Representing a diverse cross-section of Australia's technology sector, from software companies to VC firms and advisors, the TCA has unique insight into the diverse implications of cyber security regulations for the full spectrum of Australian technology companies and the broader ecosystem.

Strengthening Australia's cyber security regulations

Cyber security is a broad and dispersed area, with a range of different departments, agencies and commissioners undertaking regulatory activity and a number of different government departments conducting policy development and consultations in related areas. While these characteristics are not unique to the Australian regulatory environment, we believe that the current regulatory system would benefit greatly from clarification of roles and responsibilities and the identification or creation of a strong leading regulator.

However, in the absence of a single regulator, we believe that this consultation being framed around the incentivisation of voluntary cyber security measures will increase business engagement and guide a uniform approach to the key areas for action. We agree that these measures, while voluntary, have to be engaging, accessible for businesses of varying sizes and industries, and designed in consultation with industry.

In order for this to be done effectively, and in line with other regulatory settings and policies currently in development, we advocate for a principles-based approach to the development of these settings.

As the TCA, we recommend the adoption of the following design principles in regards to Digital Economy regulation:

- **Efficiency:** does the design of the regulation achieve its stated regulatory and policy objectives in an efficient manner, and without imposing unreasonable cost on any of regulators, industry or consumers?
- **Proportionality:** is the approach specified in the regulation commensurate with the value and risk of the opportunity being regulated, and does it target regulation to activity of concern, whilst allowing legitimate activity and new services to be introduced without undue restrictions?
- **Responsibility:** does the regulation allow for the safe introduction of new products and services, and does it respect the rights and responsibilities of consumers?

With these principles in mind, we have the following comments on the proposed strategies for the key areas for action.

Governance standards for large businesses

We are generally supportive of the development of voluntary standards for large businesses as outlined in the Discussion Paper. We recommend the standards should:

- be based upon, or able to be explicitly mapped to relevant global standards (such as ISO 27000 series),
- clearly define the qualifying criteria of businesses the standards would relate to, and
- be accompanied by appropriate implementation guidance and education programs that can also influence smaller businesses who are potentially (or should ideally be) in the process of establishing good cyber security risk management frameworks.

We strongly support the need for these standards and surrounding materials to be co-designed with industry to ensure consistency in language and approach, and to ensure the standards proportionately address the level of risk large businesses deal with when it comes to cyber security. We also believe that these voluntary standards will have a flow-on impact on smaller businesses should a principles-based approach be taken in the design and communication, as they could become a tool smaller businesses look to to guide the development of these practices.

Minimum standards for personal information

Our members take the collection, use and management of personal information very seriously. This is because they primarily offer fee- for- service or subscription models. If customers did not have trust in the way data was collected and used, they would end their subscriptions or not pay fees, jeopardising the company's business model. This means TCA companies already have in place very strong data governance standards around data collection and use, particularly for personal information, which in many cases take a more cautious approach than is required by Australian law.

We appreciate that not all businesses may have these practices in place, or have as deep a knowledge of data governance as tech sector firms. We can see value therefore in defining a Plain English minimum standard for dealing with personal information.

We do not support doing this via an enforceable code under the Privacy Act. That is because it is most likely to be small businesses who do not currently have data governance policies in place. Many of these businesses are exempt from the Privacy Act, and therefore would not be covered under this approach. Larger companies that are covered are already subject to higher standards imposed by the General Data Protection Regulation (GDPR) or set forth in their own internal policies. Setting a lower standard via the code is unnecessary and could complicate compliance with higher standards if the minimum standards specified different approaches on the same issue.

We therefore recommend the development of minimum standards, implemented through a purpose-built standard or code, which are aligned with global standards. They should apply to all business sizes.

These minimum standards should provide companies with clear guidance on where to focus their efforts and explain why. By way of example, the Australian Signals Directorate's Essential 8 could form the foundation for a minimum standard. It has a number of features that could assist in this respect (including the tiered maturity model and existing implementation guidance). However, this would and should be complemented by:

- consideration of how these standards can evolve over time, and how they currently and will in future align to equivalent guidance and processes in other countries (including those published by NIST, the UK NCSC, the Cloud Security Alliance and Center for Internet Security), and
- having regard not only to the technical aspects of cyber security (technical risk management), but the equally important human and behavioural aspects (human risk management), including the need for education and training.

Responsible disclosure policies

We support the development of responsible product disclosure policies and believe this has benefits to both businesses and consumers alike.

We see a voluntary responsible product disclosure policy as having the potential to have a similar impact across Australian businesses to those outlined for other measures in the Discussion Paper and covered elsewhere in this submission; however, we believe that the policy should be transparent about the desired outcome of coordinating and providing best practice disclosure standards.

Key considerations in the development of such a policy include:

- **Clearly defining intended outcomes:** disclosure policies can have many key outcomes including but not limited to gathering intelligence on vulnerabilities, responding to or measuring occurrences of incidents, or maintaining good communication practices with vendors or affected entities. Clearly defining the intended outcome of the responsible disclosure policy will build trust and, we believe, increase uptake of such a standard.

- **Reporting timeframes:** ensuring recommended time frames for reporting are proportionately applicable to incidents of varying risk and intended outcome of the policy.
- **Treatment of data gathered under the policy**: alongside clarity of intent, we believe it is also necessary to be clear about how information gathered under the policy will be used to strengthen analysis, how the public and private sectors will balance reporting obligations with incident response, and how this data will encourage transparency, facilitate public-private and interagency coordination and interact with existing obligations and policies regarding disclosure.

We also recommend the Government limits responsibility for reporting only to the compromised entities. As a rule, vendors and third-party service providers should not be required to report cybersecurity incidents to the Australian Government that have occurred on their customers' networks. Without this rule, numerous challenges to normal business operations would be unnecessarily created, including disclosure of potentially confidential business information which may also breach contractual obligations. This policy should ensure it does not operate in competition with existing processes or requirements at a business level, which can be done by developing such a policy in consultation with industry.

Voluntary health checks for businesses

While we agree that to-date Department-run communications campaigns have not been sufficient in raising the standard of cyber security practices or literacy, we see no harm in the proposed campaign for voluntary health checks. We recommend first lifting lower-level cyber security literacy across small businesses.

While it is critical that messaging is simple, we would encourage a "framework" or "principles" centred campaign to encourage attitudes to cyber security that are more sustainable and build better business practices in the long run. We believe an "always on" attitude to cyber security is necessary for increasing capability uplift, which could then work in a way that is complementary to some of the proposed approaches to larger or later stage businesses.

The Discussion Paper aper sets out a systemic approach to addressing the cyber security landscape in Australia and believe that with continued industry engagement, Australia's ambitious targets of having the best Digital Economy in the world can be realised, supported by regulation that is efficient, proportionate and responsible.

We appreciate the opportunity to contribute feedback to the ideas proposed in this submission and look forward to ongoing dialogue.

Yours sincerely,

Tech Council of Australia
www.techcouncil.com.au

Kate Pounder
CEO, Tech Council of Australia
e: [redacted]
m: [redacted]