CYBERUNLOCKED

50 Yeo Street
Neutral Bay NSW 2089
Australia
Phone: 1300 901 835
E-mail: [redacted]

15 August 2021

The Hon. Karen Andrews, MP
Minister for Home Affairs
Department of Home Affairs
Australian Government

Re: Submission to discussion paper - Strengthening Australia's cyber security regulations and incentives

CyberUnlocked appreciates the opportunity to provide input to the discussion paper, *Strengthening Australia's cyber security regulations and incentives*. We congratulate the Australian Government on its leadership towards uplifting the cyber security of Australia's digital economy to date.

At CyberUnlocked we provide managed cyber security primarily to small and medium sized Australian businesses. Our mission is to build long-term cyber resilience for businesses through incremental small steps. We strongly believe that all small and medium sized Australian businesses deserve to have good cyber safety without the worry or expense of employing more staff.

We support the three areas the Government has highlighted in the paper for voluntary and regulatory measures. We welcome these efforts to reduce the social and economic impacts of cyber security incidents to Australia's digital economy. In our submission we have made observations and recommendations directly related to specific sections of the paper.

Recommendations

Recommendation related to Section 2: Mandatory standards are a must to stimulate the investment needed in upgrading Australia's cyber security

Our view is that cyber security is a team sport. The investment in cyber security must be treated as a public good that benefits all of society but whose commercial returns are difficult to measure by individual entities. If all organisations apply a minimum standard, the resilience and security of the entire nation improves.

We agree with the assessment within your paper that negative externalities and information asymmetries are contributing to the need for the government to take action to encourage businesses to better manage cyber risk. Our experience suggests, insufficient incentives to have

good cyber security practices, has allowed for discrepancies to emerge between organisations of similar sizes and in similar industries. This is particularly evident in the small and medium business sector.

With the increasing interconnected supply chains and large proliferation of cloud applications leading to negative externalities, our view is minimum mandatory standards need to be in place for all organisations to raise the cost for an attacker to target an Australian organisation. As noted in your paper there is evidence that UK organisations reported improvements to their cyber security as a result of the introduction of General Data Protection Regulation (GDPR). There is also anecdotal evidence observed in the United States from the recent introduction of the Cyber Security Maturity Model (CMMC)[1], where a shift was made from self-assessment to external audit of cyber security compliance to raise the overall cyber security of their Defence Industrial Base.

Recommendation related to Section 5: Cyber security code under the Privacy Act is an effective way to increase the uptake of cyber security standards in Australia

By international standards, we commend the importance Australia's current regulatory environment places on cyber security and data privacy through the Privacy Act 1988, Australian Consumer Law and Corporations Act 2001. The over 51 Commonwealth, state and territory laws that create or could create some form of cyber security obligation for businesses, clearly indicates an intention by the government at all levels to strengthen cyber security requirements.

Our view is that a single law that governs cyber security and data privacy expectations across the whole economy supported by clear incentives and enforcement would provide certainty to businesses and eventually reduce the cost to implement cyber security controls. A good example of this type of approach is the GDPR, that provides clarity, consistency, and enforceable rights across the EU to establish a baseline for data protection and privacy.

By extending the Privacy Act to include technology businesses that have revenue less than $3 million and implementing a single cyber security code under the Privacy Act, there is an opportunity to lift the overall cyber security standards in Australia and improve the resilience of the digital economy. Creating one set of minimum rules for which businesses must adhere, has the benefit of ensuring businesses are bound by the same principles and benefit from the same opportunities, regardless of their industry or state in which they are registered. It also ensures, businesses have a certainty to build the digital assets of the future based on a single set of principles.

As organisations use and manage personal information in different ways, our view is that protection of this information requires having the right controls for the business rather than a set of mandated technical controls. Providing a set of minimum technical controls could create a tick-the-box culture and false sense of security. We therefore do not suggest prescribing a set of technical controls as part of a cyber security code. Rather a principles-based approach that is periodically updated would enable organisations to assess their cyber risk and take appropriate actions to keep personal information secure.

[1] Office of the Under Secretary of Defense for Acquisition & Sustainment, *Cybersecurity Maturity Model Certification*, available at: https://www.acq.osd.mil/cmmc/draft.html

Recommendation related to Section 9: A cyber security health check program for small business needs to include a focus on prescriptive controls aligned to business risk

We support the option presented in the paper to adopt a cyber health check program for small businesses. We fully agree with the deduction in the paper that small businesses face the challenges of limited time, limited funds, and limited cyber security expertise. A well-designed program awarding a small business with a trust mark would provide assurance to the businesses' customers as well as their suppliers that the business meets basic cyber security standards.

Our view is that success of such a program will depend on the adoption rate as well as the ability of the controls to greatly reduce cyber-attacks and data theft from small business. Incentives such as tax deductions are required to ensure all businesses have equal access. Below we have provided three recommendations that we believe would strengthen the implementation of a cyber security health check for small businesses.

a) Prescriptive controls
   Our experience shows, small businesses do not have the expertise or investment to adhere to a principles-based approach to cyber security. Therefore, prescribing minimum technical controls that a business must incorporate to meet the health check removes the ambiguity and provides clarity on the steps a business needs to take to achieve compliance. While we believe it may not be realistic to mandate the Australian Signals Directorate's Essential 8 for all small business, a subset of these controls could be mandated for businesses that need controls. Steps such as enabling multi-factor authentication, regular application and operating system patching and restriction of administrative privileges are often free to turn on and can go a long way in preventing many common types of cyber-attacks. Humans are still a weak link in cyber defences and an approach that can incorporate free cyber education for small business owners and employees also has the potential to greatly reduce cyber-attacks on small businesses.

   The methods used by cyber criminals are continuously evolving and any prescriptive controls will need to be kept updated and evolve over time. The Australian Cyber Security Centre (ACSC) already provides excellent guidance and recommendations on technical controls for cyber security, and we would welcome the ACSC taking on a greater role within a health check program. We agree with the paper's suggestion that a health check award needs to be time-bound. Our view is that a yearly self-assessment supported by the right commercial incentives for business could maximise compliance while providing a good level of cyber protection.

b) Requirements aligned to business risk
   Not all small businesses are the same and their level of digital maturity also greatly differs depending on their industry and business model. Mandating the same prescriptive technical controls across the entire spectrum of small businesses could have limited impact. As an alternative approach, for this program to have high impact, our view is that businesses must be prescribed controls based on their industry sector, their level of digital maturity and the amount of sensitive data they hold. Insurers of cyber risk could be an industry partner the

government work with to create the guidelines to measure the cyber risk of an organisation based on their industry sector and level of digital maturity.

c) Phased implementation
Our view is that any health check program for small business needs to be designed with a decade long goal of improving the cyber security culture and thereby the cyber resilience of Australia's digital economy. We welcome the approach suggested in the paper to work with prioritised peak industry bodies to promote such a program. While this would improve the compliance in specific sectors initially, there needs to be a pathway to cover all businesses that interact with sensitive data to eventually be part of such a program. Similarly, while it may only be feasible to expect voluntary compliance in the first year or two of the program, there needs to be a path to mandatory compliance. Cyber criminals are continuously evolving and looking for any businesses with vulnerabilities, protecting only certain sectors or a subset of businesses within a sector, has the potential to push the problem to unprotected businesses.

Closing comments

CyberUnlocked looks forward to continuing engagement with the Australian Government as it works towards identifying and implementing the frameworks to strengthen Australia's cyber security. With the right regulations and incentives in place, we look forward to a reduction in the economic and social impacts caused by cyber security incidents. If you have questions in relation to this submission, you can contact me directly on [redacted] or [redacted].

Yours sincerely,

[redacted]

Sarah McAvoy
Managing Director