CYBERUNLOCKED

Discussion Paper Submission

2023-2030 Australian Cyber Security Strategy

3 April 2023

Level 25, 100 Mount St
North Sydney NSW 2060
Australia

Phone: 1300 901 835

E-mail: info@cyberunlocked.com.au

Foreword

CyberUnlocked appreciates the opportunity to provide input to the 2023-2030 Australian Cyber Security Strategy. We congratulate the Australian Government on its leadership towards uplifting the cyber security of Australia's digital economy.

At CyberUnlocked we provide consulting and 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.

We welcome the government's commitment to creating a digital environment that is safe, trusted, and secure. Cyber-attacks on organisations have far-reaching consequences, with customers often bearing the brunt of the damage in terms of compromised personal information and potential for financial loss. We strongly believe enhancing every organisation's cyber security is crucial for protecting all Australians and fostering a secure digital environment. In our submission, we have made observations and recommendations directly related to specific sections of the paper.

Sarah McAvoy

Managing Director & Founder
CyberUnlocked

Summary of Recommendations

In response to question 1, we have provided 6 recommendations that we believe should be included in the strategy to make Australia the most secure nation by 2030.

- Mandatory standards through regulation are a must to stimulate the investment needed in upgrading Australia's cyber security.
- Expand the scope of the Security of Critical Infrastructure Act to include customer data and 'systems' alongside critical assets, enhancing protection and encouraging organisations covered by the Act to prioritise individuals' data security and privacy.
- Amend company directors' obligations to explicitly include cyber security risks, with consequences for insufficient action, while providing clear guiding principles and government support to ensure a consistent, informed approach to cyber security directives.
- A single Cyber Security Act across all states and territories is an effective way to increase the uptake of cyber security standards in Australia.
- Collaborate with international partners and involve cyber insurance providers in developing a flexible, global approach to addressing ransomware payment policies, accounting for the unique nature of each situation.
- A government and industry supported cyber security certification program for small and medium businesses with a focus on prescriptive controls aligned to business, and supported by financial incentives would uplift the cyber resilience of Australia's digital economy.

Response to Question 2

Recommendation 2.1: *Mandatory standards through regulation 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.

Our experience suggests, insufficient incentives to have good cyber security practices, and information asymmetries on what is good cyber practice, have 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 regulation with clear minimum mandatory standards need to be in place for all organisations to raise the cost for an attacker to target any Australian organisation.

Recommendation 2.2: *Expand the scope of the Security of Critical Infrastructure Act to include customer data and 'systems' alongside critical assets, enhancing protection and encouraging organisations covered by the Act to prioritise individuals' data security and privacy*

It is commendable that the Australian government has taken proactive steps to protect the nation's critical infrastructure through the Security of Critical Infrastructure Act.

Considering the rapidly evolving digital landscape, it is imperative for the Australian government to consider expanding the scope of the Security of Critical Infrastructure Act. By including customer data and 'systems' within the definition, the Act can better address the increasing complexity and interconnectedness of the digital ecosystem.

Incorporating customer data and 'systems' in the legislation will not only enhance the protection of sensitive information but also encourage businesses to prioritise data security and privacy. By revisiting the Act's definition, the government can ensure that Australia remains at the forefront of cyber security, safeguarding both critical assets and the valuable data that supports them. This proactive approach will bolster national security and help build a more resilient digital economy.

Recommendation 2.3: Amend company directors' obligations to explicitly include cyber security risks, with consequences for insufficient action, while providing clear guiding principles and government support to ensure a consistent, informed approach to cyber security directives

The Australian government should consider amending the obligations of company directors to explicitly include addressing cyber security risks. By doing so, directors would be held accountable for ensuring that their organisations take adequate measures to protect against cyber threats. This heightened responsibility would encourage proactive measures, such as assessing their organisations cyber risk, implementing cyber security policies, investing in cyber security infrastructure, and promoting employee training.

To enforce these obligations, the government should consider introducing consequences, including director liability, for failing to take sufficient steps to protect their company from cyber risks. This approach would provide a strong incentive for directors to prioritise cyber security and demonstrate due diligence in safeguarding their organisation's digital assets.

To support company directors in fulfilling their expanded obligations, the government should establish clear principles that guide their responsibilities and outline best practices for protecting their company against cyber threats. By providing a framework for directors to follow, the government can ensure a consistent, informed approach to cyber security management across businesses of all sizes. This initiative will ultimately strengthen Australia's digital economy, bolster national security, and foster a culture of cyber resilience.

Recommendation 2.4: *A single Cyber Security Act across all states and territories is an effective way to increase the uptake of cyber security standards in Australia*

As the minister has stated in their foreword, Australia has a patchwork of policies, laws and frameworks that are not keeping up with the challenges of the digital age. The over 50 Commonwealth, state and territory laws that create or could create some form of cyber security obligation for businesses today, creates an environment where it is close to impossible for businesses, most of which are small or medium-sized, to accurately understand their obligations on cyber security.

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 enacting a unified Cyber Security Act that establishes a single set of cyber security standards, Australia can enhance its overall cyber security posture and bolster the resilience of its digital economy. Creating one set of minimum enforceable standards 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 the 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 organisations 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 cyber security standards. Rather a principles-based approach that is adaptable to the dynamic cyber environment out to 2030 would enable organisations to assess their cyber risk and take appropriate actions to keep data secure.

Recommendation 2.5: *Collaborate with international partners and involve cyber insurance providers in developing a flexible, global approach to addressing ransomware payment policies, accounting for the unique nature of each situation*

The Australian government should approach the issue of ransomware payments as a global concern, working closely with international partner countries to align on a cohesive strategy. Cyber security threats, such as ransomware, are borderless in nature and often have far-reaching impacts that extend beyond a single nation. Australia is already a respected voice in addressing the challenge of making the world a safer place and can leverage this voice to shape global thinking in relation to ransomware. Adopting a collaborative approach with other countries, including those in Southeast Asia and the Pacific, will lead to more effective and comprehensive solutions.

Additionally, it is crucial to involve cyber insurance providers in any discussions or decisions regarding ransom payments. Given that these providers are backed by global underwriters, their insights and expertise can help inform more balanced and well-considered policies.

It is important to acknowledge that each ransomware situation is unique, and a one-size-fits-all directive may lead to unintended consequences. Policymakers should consider developing flexible guidelines that account for varying circumstances and allow for discretion in decision-making. By adopting a collaborative, nuanced approach to addressing ransomware payments, the Australian government can contribute to a more resilient and secure global digital ecosystem.

Response to Question 15

Recommendation: A government and industry supported cyber security certification program for small and medium business with a focus on prescriptive controls aligned to business, and supported by financial incentives would uplift the cyber resilience of Australia's digital economy

Small and medium-sized businesses play a vital role in Australia's economy, contributing significantly to employment, innovation, and regional development. With over 99% of businesses in Australia being small or medium in size, they foster a diverse market, generate job opportunities for millions of Australians, and serve as the backbone of local communities, helping to drive economic growth and maintain the country's competitive edge.

Our view is that a well-designed program awarding small and medium businesses with a cyber security certification such as a trust mark, would provide assurance to the businesses' customers as well as their suppliers that the business meets basic cyber security standards. The 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 businesses. Below we have provided recommendations that we believe would strengthen the implementation of a cyber security certification program for small and medium businesses.

Prescriptive controls

Our experience shows, small and medium 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 certification 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 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 business owners and employees also has the potential to greatly reduce cyber-attacks on small and medium businesses.

Guidance and education

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 certification program.

Compliance

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. Introducing a government-backed trust mark for businesses that meet minimum cyber security requirements would instil confidence in consumers who seek assurance their data is protected.

Financial incentives

Small businesses face the challenges of limited time and limited funds. Incentives such as tax deductions, grants and subsidies are required to ensure all businesses have equal access. Further, rewards to businesses that meet the certification could include, cyber insurance backed by a government guarantee, so businesses that have done their bit to uplift Australia's cyber security standards, are provided the support to quickly recover from cyber-attacks.

Requirements aligned to business risk

Not all 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 and medium 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.

Phased implementation

Our view is that any certification program for small and medium 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. The government can 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.

CYBERUNLOCKED

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 better protection and enhancement of our collective cyber resilience, both in Australia and in our region.

Level 25, 100 Mount St
North Sydney NSW 2060
Australia

Phone: 1300 901 835

E-mail: info@cyberunlocked.com.au