Steadfast
THE STRENGTH YOU NEED

11 April 2023

The Expert Advisory Board of
2023-2030 Australian Cyber Security Strategy

Dear Sir/Madam,

Re: Submission to the 2023-2030 Australian Cyber Security Strategy discussion paper

I am writing to provide input on behalf of Steadfast Group for the Australian cybersecurity strategy discussion paper. As a leading insurance business in Australia and a member of the ASX Top 100, we understand the critical importance of effective cybersecurity measures in protecting our customers' data, our business operations, and our national security.

We share and appreciate the goal for Australia to become the most cyber secure nation by 2030, and we believe that a strong national cybersecurity strategy is essential in achieving this goal. As a company with significant experience in risk management, we are committed to ensuring the highest standards of cybersecurity across our operations, and we understand the importance of collaboration between industry, government, and other stakeholders in achieving this goal.

Based on our extensive experience in the insurance industry and our commitment to ensuring the highest standards of cybersecurity, we would like to offer our insights and recommendations to help shape an effective national cybersecurity strategy that meets the needs of our society and economy.

Thank you for your consideration of our input, and we look forward to seeing the final strategy document.

Your sincerely

Alexander Moskvin
Head of Cybersecurity

Steadfast Group Limited
ABN: 98 073 659 677

Level 4, 99 Bathurst Street, Sydney NSW 2000
PO Box A980, South Sydney NSW 1235
T +61 (02) 9495 6500 **W** steadfast.com.au

1. **What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?**

   To achieve the goal of making Australia the most cyber secure nation by 2030, we believe it is important for the government to consider declaring cybersecurity as a public good or "res communis." By doing so, it would demonstrate the government's commitment to ensuring a basic level of protection for individuals and businesses in Australia. This could include establishing general cybersecurity services that are available to all businesses and individuals in Australia, such as providing access to basic cybersecurity training and resources, promoting best practices in cybersecurity, and creating awareness campaigns to increase understanding of cyber risks and how to mitigate them. Additionally, we suggest that the strategy prioritize collaboration between industry, government, and other stakeholders, both within Australia and internationally, to share knowledge and resources and to develop a coordinated response to cyber threats.

2. **What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?**

   a. **What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?**

      To improve mandatory operational cybersecurity standards across the economy, we believe that a combination of legislation, regulation, and further regulatory guidance may be necessary. Specifically, we suggest moving from a "common sense" approach to more prescriptive regulation in cybersecurity, where rules are specific and punishments for non-compliance are immediate and imminent, similar to how traffic rules are enforced with speed cameras. The Essential Eight is an excellent example of moving in this direction, as it provides a list of specific controls that businesses and cybersecurity professionals can use to define actionable strategies.

      Additionally, we suggest implementing mandatory cybersecurity requirements for high-impact systems and processes. For example, organisations managing more than a specific number of records of highly sensitive personal data could be required to achieve Essential Eight maturity level 2, or OT systems that impose health and safety risks for more than a specific number of people could be required to have specific controls in place. We believe that these measures would help to ensure that the most critical systems and processes in the economy are adequately protected against cyber threats, while still allowing for flexibility in implementation to account for the diversity of businesses and industries in Australia.

   b. **Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?**

   c. **Should the obligations of company directors specifically address cyber security risks and consequences?**

      We believe that the existing obligations of company directors are sufficient to address cybersecurity risks and consequences. Directors have a duty to look after all business risks, including cybersecurity risks, and are already required to act in the best interests of the company and its stakeholders. However, we also believe that the mentality and corporate culture around cybersecurity risks may start to change once there are examples of the administration of justice related to cybersecurity risks. While there have been cases of negligence in cybersecurity during the recent months, there have been few personal actions taken against company directors and top management for these failures. Therefore, we believe that enforcement and accountability are key to ensuring that companies take cybersecurity risks seriously and that directors are incentivized to prioritize cybersecurity as a critical business risk.

d. Should Australia consider a Cyber Security Act, and what should this include?

While we believe that the intention behind a Cyber Security Act is positive, we believe that it is more important to focus on actions rather than words. Any legislation should be carefully considered and should include specific measures to improve cybersecurity across the economy. However, we also believe that it is important to prioritize the implementation of existing frameworks and laws, before considering new legislation. Ultimately, we believe that a comprehensive and proactive approach to cybersecurity, backed up by effective enforcement and accountability, will be more effective than any new legislation alone.

e. How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?

To reduce the regulatory burden on businesses, the government can establish a centralised repository of compliance assessments. The repository should have a set of standard profiles to address common regulatory requirements, and each company should maintain its information required to complete applicable compliance profiles. When the company is requested to submit an assessment by its counterpart, they send a secure link to their profile in the repository. The compliance profiles/questionnaires are checked and approved by regulators. Participation is voluntary and paid to cover the register maintenance costs. This will allow companies to free up significant amounts of compliance and cybersecurity resources, redirecting them towards value-added tasks. It will also reduce the distribution of corporate confidential and sensitive information through email and other unprotected media.

f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by:

(a) victims of cybercrime; and/or

While it is understandable to discourage the payment of ransoms and extortion demands by cyber criminals, mandating this could potentially do more harm than good. If victims of cybercrime are prohibited from paying ransoms, they may feel compelled to keep the attack hidden or attempt to deal with the situation themselves, potentially leading to further damage. Instead, the Government should focus on strengthening cybersecurity measures and increasing awareness to prevent such incidents from happening in the first place.

(b) insurers? If so, under what circumstances?

The Government should consider prohibiting insurers from paying ransoms and extortion demands by cyber criminals, as this may create a false sense of protection. However, there may be certain circumstances where insurers should be allowed to pay ransoms, such as when it is the only option to prevent harm to human life or if there is a clear public interest in doing so. Any exceptions to the prohibition should be carefully defined and limited to prevent abuse.

g. Should Government clarify its position with respect to payment or nonpayment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

3. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?

The focus on the geographical region may not be the most effective approach in the digital world. Instead, Australia could collaborate with countries such as Singapore, South Korea, and the United Arab Emirates, as they have similar economies and types of cyber threats. These countries could form an international group with a common cybersecurity agenda, sharing information and best practices to improve regional cyber resilience and better respond to cyber incidents. Additionally, Australia can lead these efforts to promote international norms and standards for responsible state behaviour in cyberspace to reduce the risk of cyber conflicts and enhance global cybersecurity.

4. **What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?**

5. **How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?**

6. **How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?**

7. **What can government do to improve information sharing with industry on cyber threats?**

8. **During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?**

9. **Would expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?**

   Requiring mandatory reporting of ransomware and extortion demands would not improve public understanding of these types of cybercrime. Instead, it would likely increase speculation in social and regular media and distract businesses from effective incident response.

10. **What best practice models are available for automated threat-blocking at scale?**

11. **Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?**

    In addition to the broader STEM agenda, Australia may benefit from a tailored approach to uplifting cyber skills. The current school curriculum may not effectively prepare students for emerging areas like cybersecurity, which require creativity, pragmatism, and strong out-of-box thinking. To promote this different type of thinking, there should be greater support for Math/STEM Olympiads and other events that focus on problem-solving and critical thinking.

12. **What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation/n?**

13. **How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?**

    a. **Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?**

       Agreed, having a single reporting portal for all cyber incidents and harmonising existing requirements would simplify the reporting process for organisations and reduce the burden of reporting separately to multiple regulators. It would also allow for a more coordinated response from regulators and government agencies to address cyber incidents in a timely and effective manner.

14. **What would an effective post-incident review and consequence management model with industry involve?**

15. **How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?**

    Australia should consider creating an Emergency Cyber Help Service to provide assistance to individuals and businesses affected by cyber incidents. This service would be similar to emergency services like police, ambulance, and firefighters, and would offer support for responding to and recovering from cyber attacks. By providing this service, individuals and businesses would feel more supported and less alone in dealing with cybercrime. Additionally, the service should be subsidised to ensure it is accessible to all who need it.

16. **What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?**

17. **How should we approach future proofing for cyber security technologies out to 2030?**

18. **Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?**

19. **How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?**

20. **How should government measure its impact in uplifting national cyber resilience?**

21. **What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?**