AUSTRALIAN Cyber Collaboration Centre

Australian Cyber Security Strategy

Discussion Paper Submission

13/04/2023

Contents

1 Executive Overview

The Australian Cyber Collaboration Centre (The Centre) is a not-for-profit, member-based organization dedicated to promoting and ensuring cyber resilience across the Australian economy. We appreciate the opportunity to provide our input for the Australian Government's 2023-2030 Australian Cyber Security Strategy discussion paper. As an organization committed to enhancing the security and safety of Australia's digital infrastructure, in particular small to medium enterprises, we believe that the government's new strategy will be a significant step towards achieving this goal.

The government's new strategy should provide a clear roadmap for strengthening Australia's cybersecurity posture. We appreciate the comprehensive approach that the government has taken in addressing the many challenges facing the country's cybersecurity landscape and the broad consultation being undertaken. We are particularly pleased with the focus on collaboration and partnership, as this is at the core of what we do at the Centre. By working together with government, industry, and academia, we believe that we can achieve greater cyber resilience across the Australian economy.

At the Australian Cyber Collaboration Centre, we believe that cybersecurity is not just an issue for the government or the private sector alone; it is a shared responsibility that requires a coordinated effort from all stakeholders. We are encouraged by the government's recognition of this fact and the emphasis it has placed on the need for a whole-of-nation approach to cybersecurity. We are committed to playing our part in this effort and look forward to working with the government and other stakeholders to achieve our common goals.

The Australian Cyber Collaboration Centre fully supports the government's development of a new strategy on cybersecurity. We believe that this is a critical step towards enhancing the resilience of Australia's digital infrastructure and protecting the country from the growing threat of cyberattacks. As an organization dedicated to promoting collaboration and partnership in the cybersecurity landscape, we are eager to play our part in achieving these goals and look forward to working with the government and other stakeholders to make it happen.

Matt Salier

Chief Executive Officer

Australian Cyber Collaboration Centre

2 Document Overview

Purpose

This paper consolidates the views of the Australian Cyber Collaboration Centre; a not-for-profit member-based organisation established to build cyber security capacity in the Australian economy to secure our nations digital future. With a vision to ensure cyber resilience is accessible, affordable, and achievable across the Australian economy we are deeply committed to continuing to play a key role in the nations approach to cyber security and the responses in this paper represent the broad views of a large section of our membership.

Executive Summary

It is becoming increasingly clear that digital technologies are becoming an essential part of our lives in every possible way. However, this also means that any disruption or hazard to digital systems can have a direct impact on our safety, security, and overall wellbeing as a nation.

Simultaneously, the merging of digital technologies with physical and social aspects of our lives also presents numerous opportunities for individuals, businesses, communities, government, and society as a whole. To make the most of these opportunities and reap the benefits, it is essential to build a society-wide resilience to cyber risks.

This means working together to prepare for, withstand, recover from, and adapt to the risks that come with the digital age. By building a whole-of-society approach to cyber resilience, we can better prepare ourselves and our systems for any challenges that may arise and continue to thrive in this digital era.

In this response submission, we have brought together these themes above along with key insights from our members with comments to the specific questions outlined in the Discussion Paper presented by the Expert Advisory Board.

3 Summary of Responses

3.1 Core Policy Areas

We firmly believe that the core policy areas that have been identified are crucial and hold the key to implementing important strategic changes at a national level. It is critical for the government to play an active role in setting clear and robust policies that can bring about effective change and make a difference in the long run.

To this end, we strongly advocate for the implementation of a new Cyber Security Act that outlines clear legislative obligations and standards across industry and government. Such an act would be welcomed across Australia, as there is a need to declutter and simplify the cyber landscape for non-cyber practitioners. This is especially important as the scope of people and industries affected by cyber risks continues to increase rapidly. Our specific focus on SME's constantly reinforces this need to us.

We also strongly recommend that customer data and 'systems' be included in the definition of critical assets of the SOCI Act. This would help ensure that the powers afforded to the government under the act can extend to major data breaches and not just operational disruptions.

Furthermore, we believe that strengthening our international leadership and relationships is critical. Cybercrime and threats have no borders, and it is imperative that we have strong partners internationally to tackle these complex issues. Building on the recently formed multilateral security pacts, such as AUKUS and QUAD, will serve the nation well. These pacts offer prepositioned allies to aid a speedier collective response and richer intelligence and information sharing.

In conclusion, the Australian Cyber Collaboration Centre believes it is essential that we take proactive steps to address the evolving cyber risks and threats facing our nation. By implementing the policy recommendations outlined above and working together nationally and internationally, we can build a more resilient and secure digital future for all.

3.2 Potential Policy Areas

As Australia works to develop its national cyber resilience strategy, it must carefully consider and explore potential policy areas. One crucial area is the improvement of public-private mechanisation for cyber threat sharing and blocking, as it has the potential to deliver significant scalable uplift. Additionally, addressing the skills and talent pipeline is a key priority, given the global cybersecurity skills gap, which is estimated to be 2.72 million in 2021 and 3.4 million in 2022.

To address this challenge, it is important to recognize that it is not only about the headline supply and demand gap, but also the technical versus soft skills gap, diversity gaps, and sectoral gaps. While STEM disciplines are essential, it would be short sighted to predicate the national cyber workforce on the STEM skills pipeline alone. Complementary skills pipelines that feed into non-technical cybersecurity career pathways such as policymaking, governance, risks and compliance, social and cultural engineering, psychology, and cyber diplomacy must be outlined in the strategy.

The strategy should also consider the creation of national frameworks to respond to major cyber incidents, aligning with the whole-of-society, multi-level coordination and response framing defined in the National Strategy for Disaster Resilience. Additionally, the strategy should give attention to strengthening the cyber resilience of marginalized stakeholders such as SMEs and civil society organizations and establish sector focused CIRTs to provide incident response to non-critical sectors.

Finally, a human-centric focus should be articulated in the strategy to elevate the human-factors in cybersecurity, recognizing that they remain the key weaknesses and vectors exploited in cyber-attacks. The previous strategy recognized the responsibilities of community stakeholders, but the new strategy must spell out mechanisms and avenues for engagement of community stakeholders in the co-production of cyber resilience. This may involve training and capacity-building for marginalized population groups, intelligence sharing, first response, and recovery interventions for socio-technical cyber threats. Ultimately, the goal of the strategy should be to create a safe, trusted, and secure environment for Australians.

3.3 Detailed Responses

3.3.1 What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030? (Question 1)

As the technology landscape evolves, the Australian Cyber Collaboration Centre recognizes the challenge faced by the Expert Advisor Board in developing a relevant cybersecurity strategy for 2023-2030. We believe that the growth of cloud computing, the rise of the Internet of Things, and the evolution of artificial intelligence will have a significant impact on cybersecurity. It is crucial that the government remains vigilant in identifying and addressing these threats to protect Australia's digital infrastructure and includes mechanisms in the strategy to act with agility and purpose.

These four areas are of particular note:

1. The evolution of Web3 technology has the potential to revolutionize the way we think about cybersecurity. At its core, Web3 is characterized by decentralized governance, distributed architectures, and ledger technologies, and interoperable trust less systems. This decentralized nature of Web3 will have major implications for data ownership and privacy, user identity, compliance, and regulation. Additionally, law enforcement will need to adapt to this new technological landscape. The Expert Advisor Board should consider these potential impacts and work to develop strategies to address the unique challenges posed by Web3 technology.
2. In today's world, global information assemblages comprise critical nodes which afford specific countries asymmetric control and leverage towards geostrategic outcomes. Ensuring a sovereign and assured capability to counter cyber threats requires understanding the levels of exposure and dependence on these key control nodes and employing technical and diplomacy instruments to address the associated risks. The Expert Advisor Board should consider these potential threats and work to develop strategies that can account for these risks. By working to secure these critical nodes and addressing these associated risks, the Expert Advisor Board can help ensure the security and resilience of Australia's digital infrastructure.
3. Artificial intelligence (AI) is poised to have a significant impact on cybersecurity in the near future. AI, with its generative and autonomy capabilities, is anticipated to become a critical layer and core fabric of the cyber infrastructure. However, securing the cyberspace will require addressing the concerns associated with adversarial AI and putting in place relevant compliance and accountability mechanisms. The Expert Advisor Board should consider the potential implications of AI on cybersecurity and work to develop strategies to address the associated risks.

4. The complexity of cybersecurity risks is increasing, and recent globalization and digital transformation developments mean that risks cascade quickly not only across sectors but also across countries. Managing cyber risks requires a broader national risk management strategy that accounts for the complex interactions between different systems. Tools such as complex systems modelling can help map out and operationalize risk management plans in a way that recognizes and accounts for these complex interactions. The Expert Advisor Board should consider these complex risk landscapes and work to develop strategies that can account for these complex interactions.

Establishing appropriate Governance and compliance frameworks is crucial to ensure that emerging technologies comply with relevant regulations and standards. As new technologies continue to emerge, it is essential to have a regulatory framework in place that outlines the requirements for security and privacy, ensuring that technology is developed with these requirements in mind. This will help ensure that businesses are aware of the regulatory requirements for their industry, which will help them avoid potential legal issues and protect their reputation. Additionally, having a regulatory framework in place will provide a level of assurance to customers that their data and privacy will be protected.

Incorporating 'secure by design' in the development process of new technologies is crucial to ensuring that 'security' is an integral part of the technology rather than an afterthought. 'Secure by design' means that security is built into the development process from the start, rather than being added as an afterthought. This approach ensures that security is an integral part of the technology, and not something that is bolted on at the end. By building security into the design process, businesses can reduce the likelihood of security breaches and mitigate the impact of any breaches that do occur. Additionally, by adopting this approach, businesses can demonstrate to customers that they take security seriously, which can help build trust and protect their reputation.

Engagement and collaboration with security professionals who can assist in identifying potential security risks and controls is critical. This can be achieved through workshops and the Cyber Security Cooperative Research Centre (CRC). By working with security professionals, businesses can identify potential security risks and develop controls to mitigate those risks. This approach can help businesses stay ahead of the latest security threats and vulnerabilities, ensuring that they are prepared to deal with any potential breaches. Additionally, working with security professionals can help businesses identify best practices and implement them in their own operations, which can help improve their overall security posture. Finally, by collaborating with other businesses and organizations, businesses can benefit from shared knowledge and experience, reducing the overall cost of cybersecurity.

Beyond future technology incorporation it is critical for government policies to support small to medium enterprises (SMEs) through a range of assistance programs to guide them through the

complex cybersecurity landscape. SMEs often have limited resources and knowledge when it comes to cybersecurity, making them vulnerable to cyber threats and rapidly changing threat vectors. Cyber-attacks on SMEs not only compromise their own data but also put their clients and partners at risk. The impact of a cyber-attack on SMEs can be devastating, leading to lost revenues, reputational damage, and even bankruptcy.

Government policies can help SMEs improve their cybersecurity posture through a range of assistance programs. For example, the government can provide cybersecurity training and education programs that are tailored to SMEs' needs and budgets. Such programs can help SMEs understand the risks they face and how to mitigate them, as well as how to respond in case of a cyber-attack. Additionally, the government can provide financial assistance, such as grants or tax incentives, to help SMEs invest in cybersecurity technologies and services.

Supporting SMEs through cybersecurity assistance programs also benefits the broader economy. SMEs are a significant contributor to economic growth and employment in many countries, including Australia. Therefore, it is in the national interest to ensure that SMEs are protected from cyber threats. By supporting SMEs through cybersecurity assistance programs, the government can help them to maintain their competitiveness, protect their clients and partners, and contribute to the overall economic well-being of the country.

Clear incorporation in the strategy of government policies that support SMEs through a range of assistance programs are critical to guide them through the complex cybersecurity landscape. SMEs often have limited resources and knowledge when it comes to cybersecurity, making them vulnerable to cyber threats. Supporting SMEs through cybersecurity assistance programs not only protects them from cyber threats but also benefits the broader economy. Therefore, the government should clearly outline how continued investment in and development of policies that support SMEs in their efforts to improve their cybersecurity posture.

3.3.2 Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda? (Question 11)

As a not – for – profit organization with a range of educational offerings, we recognize that developing a skilled cyber workforce in Australia requires a tailored approach beyond the government's broader STEM agenda. While STEM skills are undoubtedly important, cybersecurity demands specialized technical and non-technical skills. Technical skills include network security, encryption, malware analysis, and incident response, while non-technical skills such as risk management, policy development, and communication are equally crucial. Thus, there is a pressing need for a tailored approach that focuses specifically on developing these skills.

Fortunately, the Australian government has recognized this need and has developed several initiatives to improve cybersecurity skills. For instance, the Cyber Security Cooperative Research

Centre (CSCRC) has been established to foster collaboration between industry, government, and academia in developing cybersecurity skills and technologies. The government has also launched the Cyber Security Skills Partnership Innovation Fund, which provides funding to support the development of cybersecurity skills in Australia. Private sector and academic organizations are also involved in developing cybersecurity skills through training programs, certifications, and other resources.

To build a skilled cyber workforce in Australia, a tailored approach that focuses specifically on developing cybersecurity skills is crucial. STEM skills are essential, but they need to be supplemented with specialized cybersecurity skills to effectively combat cyber threats. Therefore, as an educational organization, we encourage the Australian government and private sector to continue investing in initiatives that specifically address the cybersecurity skills gap. By doing so, we can ensure that Australia is well-equipped to tackle the evolving cyber threat landscape.

4 Conclusion

We are pleased to participate in the development of the Australian Cybersecurity Strategy for 2023-2030 and are dedicated to collaborating with the government, industry, education, and society to further enhance our combined cyber readiness.

AUSTRALIAN Cyber Collaboration Centre

About the Australian Cyber Collaboration Centre

We are a mission-driven, not-for-profit organisation that is committed to using our knowledge and expertise to make cyberspace a better, and safer, place for organisations, corporations, agencies and institutions to do business – now and into the future.

The Australian Cyber Collaboration Centre assists business to understand and navigate the cyber specialists and ecosystem to address their specific cyber needs.

Complementing the work of organisations such as AustCyber, the Cyber Security CRC and the Australian Cyber Security Centre, rather than replicating it.

We are a central connection point for business looking to improve their cyber resilience by:

- identifying and prioritising cyber challenges.
- facilitating exercises and tests with cyber hardware and software.
- accessing world class cyber training to upskill and increase the pool of cyber talent.

We educate. We incubate ideas. We build resilience. We partner. With our strong network of national and international cyber and space partnerships, we are the only cyber centre in Australia that provides an opportunity for our education, industry and business sectors to come together.

We are committed to growing the nation's reputation as a cyber security leader that delivers smart solutions and provides economic stimulus in this new world.

For more information:

(08) 8155 5320 cybercollaboration.org.au hello@cybercollaboration.org.au