D19121776

Government of South Australia
Department for Innovation and Skills

Kendra Morony
Assistant Secretary Strategy, Governance and Industry
Cyber Security Policy, Department of Home Affairs
Email: [redacted]

Dear Ms Morony

Re: Australia's 2020 Cyber Security Strategy

The South Australian Government is engaging with business, universities and TAFE SA to develop the cyber security ecosystem in South Australia to ensure we make the most of the opportunities to advance the digital economy.

The South Australian Government has committed $8.9Million to develop the Australian Cyber Collaboration Centre (A3C). The A3C will provide critical infrastructure, including a cyber range, training facilities and office space to enable business and government to test equipment, train professionals and collaborate to address cyber challenges.

Whilst based in South Australia, the A3C is intended to provide a national focus for cyber security collaboration. The A3C will be established as a not for profit membership driven organisation. Early engagement with business and academia has resulted in eleven organisations signing an MOU to become members when the A3C is established on 1st July 2020. These organisations include: Optus, DTEX systems, Cyber Security Cooperative Research Centre, DST Group, The University of Adelaide, University of South Australia, Flinders University, the Office of Cyber Security SA Government, Aust Cyber, TAFE SA and MITRE.

With the support of these organisations we have developed the A3C mission as follows:

1. Provide access to best of breed, full spectrum cyber courses and increase the supply of skilled workers.
2. Support enterprises launch new cyber products and services to global markets.
3. Build cyber awareness and resilience in Australian corporates, SME's and government.
4. Solve real world cyber challenges through collaboration.

In achieving the mission, the A3C will be completely aligned with the national interest and will collaborate with the Australian Government to ensure the issues raised in the document, Australia's 2020 Cyber Security Strategy, A call for views are addressed. The A3C is keen to support the Australian Government develop a robust Cyber Security Strategy and provides

the following insights for consideration. We welcome the opportunity to engage further regarding the development of the strategy.

Regards

Adam Reid
EXECUTIVE DIRECTOR
INNOVATION AND SCIENCE

31/10/2019
Encl. Australia's 2020 Cyber Security Strategy Views

Level 4, 11 Waymouth Street, Adelaide SA 5000 | GPO Box 320, Adelaide SA 5001 | DX541
Tel (+61) 08 8226 3821 | Fax (+61) 08 8226 9533 | www.innovationandskills.sa.gov.au | ABN 83 524 915 929

Australia's 2020 Cyber Security Strategy

As technology advances Australian companies need to maintain pace with international competitors, lifting their cyber capabilities to ensure they can protect their assets and promote their products and services. Through engagement with several industry sectors, academia and business, the Australian Cyber Collaboration Centre (A3C) has identified four critical issues that need to be addressed to lift the cyber security capability of Australian organisations.

Critical Issues

1. Skills

   The demand for cyber security professionals far exceeds the available talent, both quantitatively and qualitatively. The South Australian Training and Skills Commission estimates there are currently around 3,500 ICT workers in South Australia that require continued training in cyber security to increase and maintain their skill base and a further 1,500 workers that will be required in the next five years.

   It has also been acknowledged that formal qualifications have lagged industry skill requirements.

   The A3C will develop a world class training ecosystem that:
   a) connects professionals with industry relevant training that is sourced locally, nationally & globally;
   b) facilitates traineeships & internships through new programs to develop industry ready professionals;
   c) conducts outreach programs into schools, training and education institutions to grow awareness of cyber as a high growth career opportunity; and
   d) supports collaboration between industry and academia to co-design or tailor courses to meet industry needs.

   This will support AustCyber to broaden the impact of activities under Action 31 of Australia's 2016 Cyber Security Strategy.

2. Critical Infrastructure

   The need to test hardware, software, policies and procedures has increased as the cyber threat continues to rapidly evolve. A pilot range was established in the South Australian Node of AustCyber as part of the Joint Cyber Security Centre (JCSC) to ensure companies could meet this need. The strong demand for services and the increase in the capability required has led the SA government to invest in A3C and develop a cyber range that will enable industry to test their products and services in a safe environment. The A3C will also support companies to identify the most appropriate test and standard for their product or service.

3. Raising awareness and capability across the supply chain

Australian businesses participating in high value supply chains such as defence, high-tech, medical technology etc, need to improve their cyber security or risk losing market position as international requirements and standards evolve. The A3C will support businesses to connect with cyber security professionals and organisations that will help them transition their cyber capability through improvements in skills, process and tools. For example, A3C will amplify the efforts of AustCyber and promote practical tools such as the Information Security Manual and the Cyber Security Small Business Program.

4. Improving the maturity of the Cyber Security Industry

The Cyber Security Industry needs to mature to ensure we continue to build our collective knowledge and expertise. The current resistance to work with competitors or share information between government, industry and academia, results in each organisation responding to new threats in isolation. AustCyber and the Australian Cyber Security Centre have supported greater communication between the Federal and State governments, business and academia however there is limited capacity and reach. A3C is seeking to increase the trust and collaboration between business, government and academia through the development of partnerships, joint research projects, and developing the talent pipeline through internships and other initiatives. The A3C will also support the JCSC to share threat information, host scenarios and incident debriefing sessions to ensure a broader segment of the business community can increase their knowledge and understanding of emerging threats.

Australia's 2020 Cyber Security Strategy Views

1. What is the view of the cyber threat environment? What threats should Government be focusing on?

    1.1. As cyber threats are becoming more sophisticated and more prevalent, the Australian Government needs to focus on threats to our national interest, critical infrastructure and personal data.
    1.2. The roll out of the NBN and the widespread adoption of technology creates greater vulnerabilities within the Australian technology network.
    1.3. The low level of awareness and pro-active management and information security across the supply chain, leave the community and the economy vulnerable to cyber-attacks.

2. Do you agree with our understanding of who is responsible for managing cyber risks in the economy?

    2.1. As citizen, business and institutional risks also contribute to government risk there is a need to work collaboratively to lower the risk threshold across all parts of the community and economy.
    2.2. The introduction of the Australian Cyber Security Centre (ACSC) and AustCyber has helped to raise awareness and share information between the Federal and State Government, however there remains a significant gap in the capability of the public, SME, industry, academia and government to address cyber threats.
    2.3. The Australian Cyber Collaboration Centre (A3C) will amplify the work of AustCyber extending its reach through the business community. Supporting government, business, industry and academia to identify the appropriate standards and to collaborate to address cyber challenges.

3. Do you think the way these responsibilities are currently allocated is right? What changes should we consider?

    3.1. Product and service providers need to be responsible for ensuring the security of information. Further guidance needs to be provided to industry to clarify which standards and frameworks are the most appropriate for their particular good or service.
    3.2. The enforcement and guidance provided through the Protective Security Policy Framework (PSPF) and Information Security Manual (ISM) has increased the resilience of Australian Government agencies.

4. What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?

4.1. Government will need to work collaboratively with other government agencies, business, academia and the community to address serious threats by providing early notifications of increased activity and technical support for incident response.
4.2. The Australian Government need to work closely with service providers in an ongoing capacity to ensure they can quickly respond to incidents. The time lag that occurs between threat identification and permission to access service providers is considered an issue relating to communication procedures rather than access control.

5. How can Government maintain trust from the Australian community when using its cyber security capabilities?

5.1. The Australian Government needs to build trust with all sectors of the community through ongoing engagement and open communication regarding cyber threats and corresponding actions.
5.2. Sharing incident information in full when it is appropriate to do so will develop trust, raise awareness and build capability. Reports such as the Incident report into the ANU data breach, that outline the incident, how it took place, how it was detected and the steps that were taken to secure the network and protect access to further information, enable institutions, business and community to learn from incidents and highlight gaps in software, policies and procedures that need to be addressed.

6. What customer protections should apply to the security of cyber goods and services?

6.1. Australian consumers expect the suppliers of goods and services to maintain the security of their information and not expose them to risk through the use of their products. The Australian Government needs to ensure businesses can meet this expectation by clarifying cyber security responsibilities and requirements.

7. What role can Government and industry play in supporting the cyber security of consumers?

7.1. To prompt behaviour change in the use of goods and services, Government and industry could provide recommendations on safe practices. Just as banks provide security tips when issuing new bank cards such as sign immediately upon receipt, do not write down passwords and do not share passwords, users of new goods and services could be provided with tips on how to remain secure when using goods and services. These could form part of the conditions of use that can be enabled through a tick box process when enabling the good or service.

8. How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?

8.1. The approach would benefit from a combination of incentives, regulation, education and promotion. The regulatory environment that is established around cyber security products and services should not be a burden to the innovation system, however it needs to reflect the increased urgency to ensure a cyber secure community.

8.2. Regulation could be combined with promotion to leverage successful consumer focussed communications strategies such as Heart Foundation tick (regulated and enforced by ACCC).
8.3. We will not suggest specific financial incentives as part of this submission as these need to be developed and modelled in detail to avoid unintended consequences, however we believe financial incentives should be a part of the mix.
8.4. Offering education to industry, academia and public sector organisations is important to enable leaders to accept responsibility for security measures, programs and, to some extent, outcomes.

9. Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?

9.1. Response to cyber incidents may be supported by technical professionals from global ICT companies that respond to similar threats elsewhere.

10. Is the regulatory environment for cyber security appropriate? Why or why not?

10.1. Until the public and company boards mature in their understanding of cyber security and demand greater assurance from companies that their information is protected, regulation will be needed to maintain appropriate levels of cyber security and provide the public with a level of assurance in the use of products.
10.2. Greater clarity is required regarding the appropriate regulation or security framework for industry to apply.

11. What needs to be done so that cyber security is "built in" to digital goods and services?

11.1. Consumer awareness can be raised through the introduction of a rating system for cyber security goods and services. Similar to the energy rating on electrical appliances a cyber security rating on goods and services would prompt consumers to make safer choices and reward suppliers for improving their cyber security.
11.2. Producers of digital goods and services need to consider the cyber security of the product, the environment and the manner in which it will be used. The A3C will provide a testing service and facility to enable developers to test their hardware, software and systems against cyberattacks.

12. How could we approach instilling better trust in ICT supply chains?

12.1. Companies that operate in the ICT supply chain need to be aware of and adhere to the appropriate standard for cyber security for their industry sector. Companies along the supply chain then need to demand these standards from their suppliers. The Government has a role in clarifying which is the appropriate standard of requirement.
12.2. Industry sectors and ICT supply chains need to share information regarding new risks and cyber threats to enable the industry to address the threats and avoid vulnerabilities at each stage of the supply chain. The A3C will provide a collaborative environment where information can be shared across competitors.

13. How can Australian governments and private entities build a market of high-quality cyber security professionals in Australia?

13.1. The Australian Government is promoting cyber security career pathways, through engagement with schools and the development of cyber security CRC's.
13.2. The A3C will support career pathways by developing a world class training ecosystem that
   a) connects professionals with industry relevant training that is sourced globally,
   b) facilitates internships to develop industry ready professionals and
   c) facilitates collaboration between industry and academia to co-design or tailor course to meet industry needs.

14. Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?

14.1. There is a lack of clarity regarding the standards for cyber security insurance products and a lack of knowledge on the part of the consumer regarding what to expect in a policy and how that might translate into an outcome for their enterprise.
14.2. There is also still an apathy regarding cyber attacks, with many SME's adopting an attitude that it won't happen to me and we will fix it at the time if it does. This attitude can be addressed by making SME's more aware of the impact of cyber attacks, the practical measures they can implement to reduce their risk and the value of insurance against major attacks.

15. How can high-volume, low-sophistication malicious activity targeting Australia be reduced?

15.1. Reduction of effectiveness of this activity is the goal. If the attractiveness or the profitability of an attack method or target is reduced, there will be a reduction in attacks against Australia over time.
15.2. Establishment of better and more communicative real-time/timely threat intelligence to all businesses would assist in allowing companies to be more resilient and make better decisions.

16. What changes can Government make to create a hostile environment for malicious cyber actors?

16.1. Creating a strong digital economy that is mature and skilled in addressing cyber threats will ensure Australia is not identified as an easy target for cyber- attacks.
16.2. Establish greater requirements for ISPs to provide more base cyber services to all users.
16.3. Establish customer edge protocol filters as default across Australia.
16.4. Ensure customers that disable, remove or customise digital products, reducing the cyber security, understand the risks and have the expertise to manage incidents.

17. How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?

17.1. Sharing information between an expanded membership of the Trusted Information Sharing Network (TISN) initiative would assist greatly.

17.2. Taking the level 1, 2 and 3 Critical Infrastructure approach, then regulating or auditing a PSPF risk-based approach, would go some way to making these essential networks more resilient.
17.3. Some capabilities could be assessed by govt, others assessed by industry on behalf of govt. Supply chain assessments are also an essential part of this need.
17.4. Ensure mandatory data breach and privacy rules are considered.
17.5. Required increase in scope or regulation around these networks.

18. What private networks should be considered critical systems that need stronger cyber defences?

18.1. Members of the Trusted Information Sharing Network (TISN) for critical infrastructure sector groups, together with those that are reliant on satellite systems for positioning, timing etc. As well as networks that contain high amounts of personal information (doctors, accounting firms and real estate agencies) or intellectual property (universities, joint facilities).

19. What funding models should Government explore for any additional protections provided to the community?

19.1. The funding approach of supporting long term collaborative research through the CRCs and short-term technology development through grants administered through AustCyber is an appropriate model.
19.2. Peak industry bodies should be encouraged to develop the cyber resilience of their industries through matched funding opportunities.

20. What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?

20.1. Existing concept of classification of data need to evolve. A reassessment is required to reduce barriers, whilst maintaining appropriate levels of confidentiality, integrity and availability.
20.2. Trusted communities should be developed where data/intelligence can be shared more openly (real-time and timely).

21. To what extend do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?

21.1. The lack of awareness of cyber security threats leads consumers to make poor choices in the products they purchase, the environment they use them and the manner in which they are used.
21.2. Producers of goods and services will respond to market forces if consumers become more aware and demand greater security. This will also be the case if company boards also demand greater understanding of cyber security risks.
21.3. Consumers need to be provided information that empowers them to choose the correct device to use appropriately in the right environment.

22. How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?

22.1. Developing the understanding of cyber security in the market place can provide Australian businesses that create cyber secure products with a market advantage.
22.2. The development of the market for cyber resilient goods and services drives market development and maturity.

23. What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?

23.1. Energy ratings on electrical goods helped consumers to make informed choices and to drive industry to develop more energy efficient products. A similar approach could be applied to cyber security goods and services.
23.2. Simple user guides that drive appropriate behaviour similar to those used by banks for the set up of credit cards could ensure cyber security practices become a part of enabling and using devices.

24. Would you like to see cyber security features prioritised in products and services?

As consumers become more connected with an increasing number of smart devices, the need to prioritise cyber security increases. Cyber security should be prioritised as part of the functionality and use of the product.