SUBMISSION

NSW 2020 CYBER SECURITY STRATEGY CONSULTATION

NEW SOUTH WALES GOVERNMENT

Introduction

Moving from digital risk to trust

Australia has a critical dependency in the digital domain and therefore on the trust and security of all digital activity. With accelerated uptake of digital technologies in response to the COVID-19 pandemic and more day-to-day activities to moving online, the data presented and its analysis is an important contribution to the reframing of the nation's approach. Focus is needed on ensuring the digital environment is secure, resilient and effective.

Australia's Digital Trust Report 2020, published by AustCyber in July 2020, argues that key sections of Australia's economy are undergoing a step-change because of rapid transition to a more sophisticated, interconnected digital environment. The Report found that digital activity currently contributes AU$426 billion to the Australian economy and generates AU$1 trillion in gross economic output, generating 1 in 6 jobs. As the largest economy in Australia that is proportionately more digitally driven, NSW makes a significant contribution to this national picture.

To underline the importance of digital trust, *Australia's Digital Trust 2020* modelled the economic impact of a four-week digital interruption to Australia's economy, such as through a widespread cyber attack, would cost the Australian economy AU$30 billion, or 1.5 per cent of Australia's Gross Domestic Product. This is estimated to be equivalent to losing 163,000 jobs. The economy-wide need for cyber security and resilience is what makes the cyber security sector Australia's true horizontal enabler.

To build and secure digital trust, Australia must continue to invest in the means to secure digital infrastructure and data to not only assure trust but to also sustain efforts to reboot growth. The NSW Government has recognised the importance of building digital trust through cyber security and importantly the need to move from a risk-based approach to an investment approach to strengthen digital resilience both within government and across the state. The June 2020 announcement that it is investing AU$240 million to bolster the state's cyber security capability and create a world leading industry[1] demonstrates this.

A globally competitive NSW cyber security industry will ultimately underpin the future success of every industry in the state's economy and consequently significantly contribute to the national economy and its global competitiveness. It promotes greater trust in Australia as a safe and desirable place for businesses to pursue digitally driven growth and provides products and services that assure the cyber resilience of all organisations.

The Australian cyber security sector is small, but quickly growing in maturity and size, with an increasing number of home-grown success stories. Australian cyber security software, hardware and services companies have joined global value chains and are establishing a worldwide reputation for high quality, deep tech, niche solutions for increasingly complex cyber risks in a highly contextual, hostile cyber-physical environment. Many of these capabilities have been and continue to be born in NSW, scaling into a wide range of market opportunities including through AustCyber's NSW Cyber Security Innovation Node, co-funded by AustCyber and the NSW Government.

AustCyber is proud to have played a significant role in the growth and improved maturity of Australia's cyber security industry and broader innovation ecosystem, now alive with a range of startups, scale-ups and mature companies across capability types. At just over 3.5 years old, we have proven that a publicly funded, non profit organisation is the right mechanism to coordinate and drive industry growth, that delivers potentially enormous benefits to the economy and to the development of sovereign capability for the nation's security.

[1] https://www.nsw.gov.au/media-releases/record-funding-for-digital-infrastructure

AustCyber's Cyber Security Sector Competitiveness Plan (SCP) and its updates, together with our Cyber Security Industry Roadmap, co-authored with CSIRO Futures and Data61, identify the key issues that the sector faces together with actions that are needed to remove barriers for growth and enhance our global competitive advantages. The reports also highlight the role that cyber security plays as a horizontal sector in enabling growth opportunities in other priority sectors and underlines the importance of greater coordination by government, industry and education institutions to effectively benefit broader Australian innovation and technology uptake.

Through a lens of cyber innovation, the SCP describes goals for Australia's cyber security sector:

- Grow a vibrant and globally competitive sector
- Export Australian capability to the world
- Australia is the leading centre for cyber security education.

Building cyber security

AustCyber's comments to the key questions posed by Cyber Security NSW

Resilience

1. *What role should industry, government and the public each have in increasing our overall cyber security resilience in NSW?*

Cyber security and the drive towards cyber resilience and trusted digital activity is a shared responsibility. Overall, government should provide leadership and coordination, to enable the finite resources of government, industry and academia to better tackle the challenges arising in the threat and operating environments and take advantage of opportunities arising from Australia, and NSW, being a trusted place to do business and sustaining our way of life. Further:

- industry is responsible for ensuring its networks and digital activities operate in a secure environment and for embracing the benefits of sovereign capability uptake and creating local innovation and capability within Australia; larger businesses can model what good looks like for smaller businesses, especially within the same sectors and market positions, and use their purchasing power to foster local innovative cyber security capabilities that quickly respond to new and emerging digital risks.

- government is responsible for working with industry to develop the legal and certification frameworks as well as standards for the practice of cyber security, to enable all organisations (public and private) to effectively operate and interoperate in ways that are resilient to cyber security threats and encourage adaptive ways to manage risk. Government is also well placed to use its purchasing power to support local cyber security capability to sustain a globally competitive cyber security industry.

- the public needs to be suitably informed, including through consistent and sustained messaging, about protecting itself against cyber security threats and be better equipped to engage online with trust and confidence. Cybercrime and cyber threats flourish in an environment where our community is vulnerable.

2. *Should the NSW Government play an involved role in increasing the individual cyber resilience of NSW citizens and business? If so, how?*

Yes. On businesses, AustCyber is working in partnership with the NSW Government and Standards Australia to address gaps in cyber security standards and guidance across key industries[2] – we encourage the next Cyber Security Strategy to acknowledge this work and support its continuance across all sectors of the NSW

[2] https://www.nsw.gov.au/media-releases/new-cyber-task-force-to-drive-standards

economy as well as deepening partnerships with other Australian jurisdictions to achieve national consistency in adoption and updating.

3. *What are the threats that the NSW Government should be focusing on and what practical steps could be taken to address these?*

As reported in *Australia's Digital Trust Report 2020* and the Prime Minister's statement on cyber threats on 13 June 2020, Australia is facing increased threats from state-based actors as well as cyber criminals. These threats are growing and with the increasing reliance on digital technologies as a result of the COVID-19 pandemic, creating digital trust through cyber resilience is more important than ever. Key ways to address the threat landscape are to further support sovereign cyber security capability development, purchasing product and services from innovative cyber security companies and investing in workplace cyber skilling.

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

Governments are well positioned to influence the pace and depth of growth, in particular through strong and innovative policies and practices in procurement and onboarding of products and services. The prioritisation of sovereign cyber security as an area for preferential procurement in governments is well timed and can be structured to enable cyber security SMEs to work with the NSW Government to ensure their products meet government requiremements, certification, integration and delivery requirements.

Delivering on a preferential approach would provide leadership across governments and in the economy, while also delivering benefit to Government. A five per cent sovereign requirement in cyber security related procurements as well as the security components of all technology procurements, for example, would unlock tens of millions of dollars in contracting opportunities – a target of 15 per cent with a commitment to grow this year on year as the industry grows is a game changer. This target would sit within an overall 25% sovereign procurement target across the NSW Government.

AustCyber's industry stakeholders also advocate the following for improving approaches to procurement:

- provide incentives and leverage methods to encourage organisations across the NSW economy to buy Australian first where possible. Other countries such as the United States and United Kingdom do this well and their natonal security as well as economies have benfited significantly.

- engage with and preference local companies in writing Government tenders for cyber security capability and put in place multi-party writing teams where project complexity requires or would benefit from multinational experience, to ensure the scopes of work have both a large and small organisation perspective. Australian cyber security companies have no chance of competing if the specifications are written in ways that automatically discount smaller and medium sized companies to tender. Scoping requirements and developing Requests for Tender should be based on requirements and problem statements, not vendor features.

- build a platform for a trusted marketplace for procurement that also supports information sharing of the use case experiences of early stage technologies.

- develop incentives that encourage investment in nurturing and supporting sovereign capability for export through global value chains. Investment in earlier stage technology will create a circumstance for evolving technology to become world class (see also *R&D and Innovation* below).

- using AustCyber's procurement sandbox concept can assist industry to rapidly upskill in supplying to government, as the majority of the sector's early stage companies are inexperienced in selling to Government as a customer. The sandbox includes developing measures for de-risking business maturity aspects of the provider by exploring the product/ service being sought in the NSW Government's technology environment. Further, this approach creates a significant opportunity to shape and collaborate on developing use cases across domains/portfolios and could also offer efficiencies in onboarding and/or implementing the cyber solution.

- overlaying AustCyber's Projects Fund methodology would provide a unique first step in facilitating the matching of Government problems and challenges to industry capabilities appropriate to respond at a Technology Readiness Level suitable to the agency's context and circumstances.

5. *How can the NSW Cyber Security Policy be improved in regard to the policy's implementation and robustness?*

The NSW Cyber Security Policy can be improved by stepping up the focus on the NSW Government bolstering local cyber security companies by sourcing sovereign capability, but also by strengthening the solid foundations in the NSW Cyber Security Industry Development Strategy for developing local capability.

In partnership with the NSW Government, AustCyber has established the NSW Cyber Security Node which is part of our national network of Cyber Security Innovation Nodes across Australia. The operations of these Nodes are being strengthened to support greater consistency, share learnings and best practice, enabling the Nodes to build on their successes and expand their reach.

AustCyber welcomes the NSW Government's announcement about the creation of the cyber security vulnerability management centre in Bathurst. This is an opportunity for the NSW Node to extend its support and collaborate regionally through this new centre to uplift cyber resilience in regional NSW and projecting new capabilities more broadly. It is also an opportunity for the Policy to extend the state's regional capability and capacity and demonstrate the practice of cyber security is needed across all parts of the state and across all industries. This will further embed and sustain cyber resilience and create jobs.

6. *How can inter-government relationships be improved to bolster NSW's cyber security posture and resilience?*

Refer question 2; developing strong sovereign cyber security capability through a vibrant and agile cyber security business sector in NSW is an investment in securing Australia's digital activities across the Australian economy. With a strong sector in NSW, the NSW Government has a tremendous resource to advise, educate and shape cyber security around Australia.

7. *What strategies should NSW Government use to lead the way in detection and response?*

AustCyber defers to others to respond to this question.

8. *How can Cyber Security NSW enable the NSW Government to be more cyber resilient?*

Addressed in responses above.

9. *How should cyber security features be prioritised in government procurement of products and services?*

The best approach for security features to be prioritised by government procurement of products and services is to adopt a 'secure by design' approach to goods and services, including the proliferation of IoT devices, as described in Cyber Security Industry Roadmap.

Workforce and Skills

10. *Are the workforce and skills initiatives in the NSW Cyber Security Industry Development Strategy addressing the skills gap? If not, what could be done better? What other initiatives could the NSW Government undertake in the area of skills and training?*

The Industry Development Strategy has been key in driving focus on the development of cyber security skills in NSW. The growth of cyber skills training and education from high school through vocational education into universities is delivering a range of courses and skills levels. There is currently a focus on national consistency in this training and education across Australia, in part led by AustCyber's work with the national TAFE network on vocational qualifications, with the Australian Computing Academy in high schools and our Student Ambassador program though our NSW Node. The next Strategy would do well to augment funding already invested by scaling and extending the reach of these initiatives across NSW to ensure consistency in employee competency and assure employer needs are met while managing overall workforce advancement.

Recognising the need for the skills gaps to be filled with students leaving courses that have the qualifications and certifications that enable them to fulfill cyber security roles quickly by matching employer requirements, AustCyber has examined a variety of cyber skills frameworks and found the US National Initiative for Cyber Education is the best available and useful by providing that necessary skills and job matching.[3] It has been developed under the auspices of the National Institute of Science and Technology in the United States and is currently going through a refresh. (See further information below in response to question 13.)

11. *In which areas do you currently lack the skills you need? What are the future skills needs in cyber security sector? What are expected skills gaps based on trends?*

AustCyber encourages the NSW Government to leverage our 'cyber security census' data under our Sector Competitiveness Plan which takes a deep dive analysis of the cyber security skills needs. We are currently working on state by state analyses within the national picture, for release later this year.

12. *How can the NSW Government help increase cyber security job opportunities and training in regional NSW?*

The development of the Bathurst vulnerability centre and encouraging partnerships and links with AustCyber's national network of Nodes is the opportunity for regional areas to commence developing job opportunities and cyber skills. Ensuring there are linkages with universities and TAFEs in the region that develop and expand training, skills and education through the NICE framework (see below) will ensure the students leave these education providers with the skills they need to deliver against job roles.

13. *How can the NSW Government, educational institutes and industry build a market of high quality cyber security professionals in Australia?*

Many of the achievements noted in this submission have leveraged and/or integrated the globally recognised National Initiative for Cybersecurity Education's (NICE) Cybersecurity Workforce Framework developed in the United States. Our engagement with larger employers in Australia, public and private sector alike, have seen uptake of our dashboard resources to use the NICE Framework as a consistent baseline for workforce planning and development as well as retention and planned mobility. This has been further enhanced by our membership on the Global Forum for Cybersecurity Expertise's Working Group D: Cyber Security Culture and Skills.

The NSW Government should note the NICE Framework's utility as a standard for skilling and workforce development, as well as the benefits of it providing a baseline for skills mobility (with follow-on benefits for applicable classes of visas and talent exchanges).

Under the current structure of cyber security in Government, it will be critical across government departments and agencies. These efforts should seek to significantly expand opportunities for cross sectoral input from industry.

TAFEs and universities also report plans for continued investment in cyber security, including in applied learning environments like training Security Operations Centres, internships and incentives for increasing enrolments. The pull through of Masters and PhD students into the economy will also start to occur, including through the incentives provided by the Cyber Security CRC. The NSW Government should also consider what more it can do to speed up the coordinated achievement of quality throughput of students into cyber security jobs including through subsidised traineeships, internships and microcredentialling.

There is clearly more that needs to be done to help achieve more certainty for students, parents, teachers, employees and employers around careers in cyber security. We welcome the opportunity for our expertise to be further leveraged for scaled, coordinated national benefit in growing efforts to further deepen the talent pipeline and workforce development.

[3] https://www.nist.gov/itl/applied-cybersecurity/nice; https://www.austcyber.com/resources/dashboards/NICE-workforce-framework

14. *How can industry best connect to inform the development of cyber security training content to ensure it is fit for purpose/targeted at existing and/or future needs?*

The value of the NICE Framework is that is most useful for both industry and skills development, thus the NSW Government adopting this framework for its workforce will ensure its own skills are current and its employees have pathways for skills and promotional opportunities, making sure their expertise remains current and up-to-date. This will also encourage businesses to follow suit.

15. *What are the barriers for NSW cyber businesses when growing their business?*

For NSW cyber security companies to grow, develop their capability and flourish so they are export ready, they need access to high qaulity business opportunities where they can validate their business models, make sure their product and service oferings are market-ready and suitable for current business and technology needs. Ensuring smaller businesses have relatively equal footing to access to government contracts is the best way to overcome growth barriers.

16. *What can NSW Government do to enable business growth and support for cyber security start-ups, scale-ups and SMEs?*

Taking responses to questions 4 and 15 further, creating an environment where startups, scale-up and established SMEs are considered for government contracts by opening up technology environments through such measures as creating a procurement sandbox. By introducing these businesses to NSW Government cyber security problems and creating an environment for innovation that encourages the new technologies to use their technology to solve these cyber problems is the best way to start supporting these businesses. Assuming support for AustCyber's sandbox concept, a further step would be to connect the sandbox to impact networks already supported by the NSW Government such as those offered by Stone and Chalk and deep technology iteration programs such as those offered by Cicada Innovations.

17. *What are the opportunities for cyber in the regional areas? What can NSW Government do to enable more regional cyber businesses?*

Addressed in responses above.

18. *How could NSW Government procurement be used to support start-ups, scaleups and SMEs and local cyber businesses?*

Addressed in responses above.

Innovation and Research

19. *What role does collaboration between the academic institutions and NSW Government have for cyber security in NSW?*

20. *What are the obstacles to research, development and commercialisation in cyber security?*

21. *How can we improve the effectiveness of the current innovation and collaboration initiatives in the Cyber Security Industry Development Strategy?*

22. *Are there specific areas of capability and technical strength that NSW should grow?*

23. *How can government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?*

In response to the above questions, AustCyber provides the following information about innovation and research.

The comparative youth of the cyber security sector means its knowledge infrastructure – the value chains, normalised ways and means of doing business and structures to sustain growth and maturity – is still forming and scaling. So too are the mechanisms for meaningful public-private partnerships and repeatable measurement of sectoral value and impact.

As has occurred with the support of sustained Government funding across decades in older sectors of the economy, we consider the development and implementation of such infrastructure, designed to the needs of Australia in the context of both the Indo Pacific and global markets, is needed to capitalise on early growth for a sustained, high value sector that delivers innovative sovereign capability.

AustCyber has undertaken research across key international locations for cyber security research and innovation systems, as well as domestically in other sectors, to identify the key elements of sectoral growth from a knowledge infrastructure perspective.

The presence of startup hubs, as well as incubators and focused accelerator programs, are critical components of building and maintaining a vibrant and globally competitive cyber security sector. The United States Department of Homeland Security and SRI International have published specific insights on the role of knowledge infrastructure in the technology transition period of commercialisation, so companies have a measurably higher rate of success in achieving access to market and growth opportunities.

Trusted vetting of cyber security solutions is also a key factor for sectoral success (achieved in the procurement sandbox concept, connected to a Government approved test lab). This underscores the technical veracity and scalability of a product or service. Further, it tests market competitiveness across the different layers of the domestic market and different contexts of international markets. In a sandbox environment, deployment simulations support better solutions integration, legacy implications and enhance benefits realisation from onboarding and sustaining new/ different technologies.

Further, a well-informed investor community that appreciates the different needs for scaling cyber security products and services – that is, confidence in the deployment of both patient and rapid capital across numerous capability types and contexts – and how to navigate global regulatory challenges is equally key to sustained scaling and growth.

Importantly, thought has been given to the merits of this infrastructure to delivering a trusted marketplace with skilled professionals and providing a valuation of the sector's significant intangible assets.

The model considers how to flexibly provide for product/ service innovation, alongside investment, business acumen and talent pipelines for workers, entrepreneurs and innovators (suppliers) and executives/managers (buyers and investors in public and private sector settings). It also considers impacts of step-change interventions, from within the sector (through technological advancement or policy/ regulatory change), or from external sources such as disruptive business models or human behavioural change.

AustCyber, along with various partners in NSW and beyond, are already investing in and building the above knowledge infrastucture. We would welcome a discussion to unpack this further, to highlight existing gaps and where themes of regional cyber security and export readiness need boosting to complement significant investments already underway within NSW, such as Western Sydney Aerotropolis and Tech Central.

Other

24. *Are there any other insights or case studies you would like to share?*

See attached for referenes on successful NSW born cyber security companies supported by AustCyber.

Examples of cyber security companies born in NSW

Bugcrowd

Founded in 2015, raised $78.7 million in venture capital
Headquartered in San Francisco, USA

Bugcrowd is a crowdsourced security platform to surface critical software vulnerabilities. It was one of the first companies to embrace and utilize crowd-sourced security and cyber security researchers as linchpins of its business model.

Dekko Secure

Founded in 2013, raised ~$10 million in venture capital
Headquartered in Sydney, NSW

Dekko Secure provides world-first technology and military-grade security to allow organisations the freedom to securely communicate, share and collaborate on sensitive information – including secure video conferencing and file sharing – without requiring app installation or complex management and infrastructure.

Huntsman Security

Founded in 1999, privately funded
Headquartered in Sydney, NSW

Huntsman Security provides security technologies to measure, report and reduce cyber risk to enable the digital transformation of governments and business to more efficient operating models, while at the same time complying with the increasing demands of legislative requirements. They were the first company to enable automated reporting and management visibility of activities under the Australian Signals Directorate's Essential Eight Strategies to Mitigate Malicious Cyber Activity.

Kasada

Founded in 2015, raised $23.9 million in venture capital
Headquartered in Sydney, NSW

Kasada foils malicious threats from login to data-scraping across web, mobile, and API channels. Its category-defining web traffic integrity solution gives internet control and safety back to humans. Kasada onboards in minutes, scales up to largest enterprises and tangibly delivers ROI across business units.

Laava.id

Founded in 2017, raised $2.5 million in venture capital
Headquartered in Sydney, NSW

Laava's intelligent, scalable stack of counterfeit prevention methods protects customers against fake items or products. Built in collaboration with the CSIRO and with funding support from AustCyber, Laava's Smart Fingerprints help to safeguard businesses against loss of market share and reputational damage. They also provide a secure alternative to QR codes, which are a highly insecure form of B2B and B2C engagement.

Secure Code Warrior

Founded in 2015, raised $51.1 million in venture capital
Headquartered in Sydney, NSW

Secure Code Warrior's platform empowers software developers to be the very first line of defence by making security highly visible and providing them with the skills and tools to write secure code from the beginning. They have customers across sectors including financial services, telecommunications and global technology companies in North America, Europe, and Asia Pacific.

About AustCyber

AustCyber is a publicly funded, private entity which commenced on 1 January 2017. Our mission is to grow Australia's cyber security sector, to support the development of a vibrant and globally competitive Australian cyber security sector. In doing so, our activities enhance Australia's future economic growth in a digitally enabled global economy and improve the sovereign cyber capabilities available to protect our nation's economy and community.

We form a part of:

- the Australian Government's Industry Growth Centres Initiative, established through the 2015 National Innovation and Science Agenda, in sectors of competitive strength and strategic priority to boost innovation and science in Australia. Industry Growth Centres are required under contract with the Government to achieve for their sector:
    - increased R&D coordination and collaboration leading to improved commercialisation outcomes
    - improved management and workforce skills of businesses
    - more businesses, including small and medium enterprises, integrated into global supply chains leading to increased export income
    - a reduction in the cost of business through regulatory reform
    - additional or indirect (spillover) outcomes;
- Australia's 2016 Cyber Security Strategy. It was through the industry consultation and development of this strategy that the concept for AustCyber was first conceived.

Our funding comes from majority Federal Government grants – funding for operations and programs, and for the AU$15 million AustCyber Projects Fund which provides grants to projects that deliver national benefit. We also receive funding under contracts with the governments of the ACT, NSW, QLD, SA, TAS, WA and the Sunshine Coast Regional Council and Townsville City Council, which we match, to deliver AustCyber's national network of Cyber Security Innovation Nodes – with the NT and VIC soon to join.

We work to align and scale Australian cyber security research and innovation related activities across the private sector, research communities, academia and within Australian governments. We are responsible for maintaining a strong supply of innovative Australian cyber security solutions and capability and have established ourselves as an independent advocate for the competitive and comparative advantages of Australian technical and non-technical cyber security capabilities.

Beyond our shores, we work with partners across many countries to develop export pathways for Australian solutions and capability. This helps the rapidly growing Australian cyber security sector tap into market 'hot spots' around the world.