Australian Information Security Association

Ms. Charlotte Wood
Director, Policy and Awareness
Cyber Security NSW
Level 23, McKell Building,
2-24 Rawson Place, Sydney NSW 2000

29 July 2020

Dear Ms. Wood,

Thank you for the opportunity to provide input on the formation of the 2020 NSW Cyber Security Strategy and to help shape its development.

The Australian Information Security Association (AISA), the peak body representing the nation's cyber security sector, supports the NSW Government's intention to develop a comprehensive, sector-wide cyber security strategy to strengthen cyber resilience within NSW.

AISA is a not-for-profit charity, established 20 years ago with the mission of educating and helping the community, industry and government to be safe online. AISA's membership is broad and extensive and includes board directors and C-Level executives through to highly technical professionals and the next generation of the cyber-security workforce.

AISA has strategic partnerships with a range of organisations and other associations to help bring together the skills required to protect Australia. Some of these partnerships include the Australian Institute of Company Directors, ASPI, Crime Stoppers, Risk Management Institute of Australia and a majority of Australia's University and TAFE sector.

AISA's annual national conference, the Australian Cyber Conference, is the largest and best-regarded event on the Australian cyber calendar, with Cyber Week and Stay Safe Online anchored around AISA's conference. Last year, the conference was attended by more than 3600 delegates from 24 countries.

In the following submission, we have made several references to questions that have been omitted. These omissions are in the interest to abide to the 4-page submission requirement. While no submissions to these questions are presented here, AISA welcomes further one-on-one consultation with NSW Cyber Security to provide further depth and context drawn from extensive membership base as the peak body representing the nation's cyber security sector.

Yours sincerely

Branko Ninkovic

Sydney AISA Chair (and on behalf of the AISA members and board)

Australian Information Security Association
ABN: 181 719 35 959
Level 8/ 65 York Street, SYDNEY, NSW, 2000
Phone: 02 8076 6012 Email: admin@aisa.org.au Web: www.aisa.org.au

Resilience

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

The government, in the interest of economic growth and prosperity, must ensure its agencies have adequate cyber security capabilities and follow industry best practices – to be pragmatic and to take the lead.

The government is encouraged to implement cyber security initiatives that will assist the industry and the public in uplifting their cyber resilience across industry sectors and the broader public. Uplift initiatives, at a minimum, must focus on education and awareness, planning, and response, and more so, the government is encouraged to provide financial support and incentives for small-to-medium businesses.

Industry and the education sector must collaboratively develop relevant, current and fit for purpose courses that are independently vetted by cyber security experts and include relevant work experience placement (paid internships) to develop highly skilled cyber security professionals.

And finally the government is encouraged to take the lead through the procurement of Australian based products and services, and be more open to, and to take up cyber security POCs (proof of concepts) to support the Australian cyber security start-up sector.

All this would lead to increased cyber security resilience, economic growth and prosperity through jobs growth and local and exportable business activity within the sector.

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

AISA supports Cyber Security NSW statement "Cyber security is critical in ensuring the NSW Government provides secure, trusted and resilient services. As the NSW Government continues its digital transformation - maintaining and enhancing our cyber security capabilities is paramount." To that effect, to support this statement, it is paramount that NSW Government plays an involved role in increasing cyber resilience. This may include, but is not limited to:

- facilitate efforts or establish a body (or program) that provides a component of planning, preparedness and rapid recovery; for example, the "slip, slop, slap" campaign
- facilitate efforts or establish a body (or program) that provides a component of planning, preparedness and rapid recovery aimed at the Small-to-Medium enterprises (SME)
- implement a voucher-based scheme in partnership with suitable qualified and approved cyber security vendors to raise awareness, educate and plan, drive uptake and maintenance of good cyber security hygiene, all of which are cost-prohibitive for small businesses and non-for-profits.

It is important to note here, that small-to-medium businesses play a significant role in the digital supply chain to larger enterprises and critical infrastructure providers. Should a small business be compromised, this could lead to further compromises and potential to cause significant damage to businesses and the economy.

(Response to questions 3, 4, 5, 6, 7, 8, 9 omitted)

Australian Information Security Association
ABN: 181 719 35 959
Level 8/ 65 York Street, SYDNEY, NSW, 2000
Phone: 02 8076 6012 Email: admin@aisa.org.au Web: www.aisa.org.au

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?

NSW Government defines cyber security as "All measures used to protect systems, and information processed, stored or communicated on such systems, from compromise of confidentiality, integrity and availability." [1]

Current initiatives are influenced by such definitions that define cyber security as orientated around systems and technology with a heavy STEM focus.

What is now more apparent is that cyber security is a much broader industry sector, beyond systems and technology and with a requirement for diverse workforce and skillsets.

The field of cyber security now also requires critical thinking, problem-solving skill and creativity.

By limiting initiatives to the fields around technical individuals does a disservice to the sector by limiting the diversity of thought. For example, cyber security awareness training is excellent, but not good enough as the effectiveness is short-lived.

Behaviour change has a longer-lasting impact and drives cultural change in an organisation. Therefore, cyber security needs people who study human behaviour, psychology, sociology, economics, and anthropology.

NSW cyber security workforce and skills initiatives would improve with a wider focus, i.e. STEAM (Science, Technology, Engineering, Arts and Mathematics) to further address any current or future skills gaps.

11. What are the future skills needs in cyber security sector? What are expected skills gaps based on trends?

Those who have human behaviour, psychology, sociology, economics, and anthropology – titles are emerging

12. What other initiatives could the NSW Government undertake in the area of skills and training?

There are two key problems:

1. The supply side is not meeting the needs of industry (for example, produce individuals who are generalists, architects, GRC, and so on.)
2. The demand side does not have an incentive to employ graduates or take on interns from the university sector.

For problem 1: see response to question 10. For problem 2:

The demand side is suppressed due to lack of incentive (financial or otherwise), and in turn, this leads to a fewer and fewer work experience opportunities for recent graduates. Graduates are currently

[1] *NSW Cyber Security Policy v1.1 (emerging Australian Government cyber security definition).*

unable to secure their first role in the industry, and hence supply and demand are impacted, and a visible break down occurs.
Initiative to build work experience opportunities include:

- assisting with (paid) internships
- reduction of red tape within government (for the government) to take on interns.
- encourage industry to take on a minimum number of interns with financial support to build and deliver internal internship programs – that provide real-world outcomes and longer-term value to help build their career in the industry

free training and short courses

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

COVID-19 has demonstrated that location is no longer a constraint, however stable, fast and reliable Internet access combined with stable power infrastructure are critical requirements to creating more cyber security job opportunities in regional NSW.

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

There is no shortage of people interested in, or currently studying cyber security. The emergence of high-quality cyber security professional will only achievable through a relevant and accredited course, relevant internship to provide work experience and an incentivised industry to develop and grow upcoming cyber security professionals. Any break in the chain (education, internship, industry) will not result in high-quality cyber security professionals, and these aspiring individuals will move out of the cyber security industry altogether.

AISA, as a not-for-profit and as the peak body for cyber security professionals and the sector should review and accredit education courses to ensure they meet the high quality demanded by industry and are relevant to the industry. The ranking for courses can be tiered based on the skill area and ability for the education provider to provide guaranteed internships while students are studying. Take, for example, the Energy Star Rating for electrical appliances, and applying the same rigour to courses based on their relevance to industry, quality of teaching content and so on.

15. 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?

We are now seeing new graduates with skills that industry is not keen to take on.

Open the AISA Executive Advisory Board (EAB) to industry to ensure cyber security training content to ensure it is fit for purpose. The EAB is comprised of CISO / CSO from across multiple sectors (e.g. retail, finance, insurance, transport, manufacturing, health etc…). They employ staff in the sector to assist in the evaluation, review and ranking of courses to ensure they meet the expectations of the industry. EAB representatives can be made available to industry, training institutions and universities.

Business Growth

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

At a high level, the primary barriers for NSE cyber businesses are:

- lack of risk appetite from larger companies; a start-up; emerging tech; with no or few client base
- lack of internal stakeholder engagement; or budget; to evaluate emerging tech; proof of concept (POC) trials
- overseas larger vendors; with a track record or a lower cost base
- cost to develop products (R&D) locally in Australia – not a barrier, more a consequence as job as lost to off-shore entities.

17. What can NSW Government do to enable business growth and support for cyber security Start-ups, Scale-ups and SMEs?

Support CyRise who is a mature start-up acceleration who has been operating in Australia for the last three years. CyRise runs boot camps for new entrepreneurs and has multiple intakes a year to help support new start-ups.

NSW government agencies should also proactively participate in proof of concept (POC) trials of new software/services from Australian start-ups. This may also extend to enabling reputable start-ups to display NSW Government logo as trialling or purchasing the product. Just performing a POC in government for Australian start-ups can be a big deal for the start-up as it displaces to potential Venture Capital (VC) a level of product/service maturity.

The government may elect to take equity in a start-up post POC and possibly prior to a purchase to help provide cashflow for the start-up, enabling the start-up to continue to build and mature their product/service.

18. (Response omitted)

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

The procurement practice of NSW government agencies should give priority to purchasing software and services from Australian cyber security start-ups.

Innovation and Research

20. (Response omitted)

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

There needs to be facilitation between industry and academia as they operate differently and have different expectations. Academia is often looking for projects that can be undertaken by PhD, hence solved within 3 to 4 years, whereas Industry is expecting outcomes which are 6 to 12 months. This can be achieved in academia via a postdoc or directly through professors.

With the downturn in international students, Universities are under pressure to increase research output and industry collaboration. Hence it is an ideal time to help the two sectors integrate research.

The government could run a number of workshops, facilitate introductions and maintain a register of projects / research for the state. While there is a Cyber Security CRC, it is limited to only 7 research partners and does not have a good track record with facilitating industry-based research.

AISA could help assist in the facilitation of sessions between academia and industry.
NSW could also introduce a grant scheme to bring greater focus to partnerships between academia and industry.

22. (22, 23, 24, 25 response omitted)

Australian Information Security Association
ABN: 181 719 35 959
Level 8/ 65 York Street, SYDNEY, NSW, 2000
Phone: 02 8076 6012 Email: admin@aisa.org.au Web: www.aisa.org.au