The Honourable Tony Burke MP

Minister for Home affairs and Cyber Security

Re: 2023-2030 Australian Cyber Security Strategy Discussion Paper Forum. Public Submission Horizon 2

Dear Mr Burke,

I note your recent appointment following this years federal election to this portfolio.

Since 2022 and Horizon 1 for the 2030 Australian Cyber security strategy, I have observed the significant progress the Australian government has made in terms of initial corrective steps, including the Cyber Security Act legislation. Positive community engagement, increased awareness of Cyber Security threats and Scams.

I am humbled with the consensus of some of my recommendations, with others in the Cyber Security community where there has been adoption in several areas.

As a background, I am a Supply Chain Professional, with over 20 years of systems deployment experience, with a background in IT, and have completed a Graduate Certificate in Customs Administration, and conducting Academic research in Cybersecurity as a joint discipline.

Enclosed are responses to some of the questions posed by the Department.

1.. What trends or technology developments will shape the outlook over the next few years and what other strategic factors should Government be exploring for cyber security under Horizon 2?

There are increasing levels of digital transformation projects, which are becoming increasingly interconnected internally within organisations and also sharing information across other businesses and government organisations.

This is increasing the surface area for potential cyber attacks, and introduces additional risks as sensitive information is shared across multiple organisations.

The Government may be able to assist by providing a framework and guidelines for organisations who share data with each other, and clearer definitions of data retention, query limits or other policies.

Higher levels of personal information and meta data are being captured by social media organisations, and there is also a pipeline of potentially identifiable and sensitive information being drawn into generative AI systems for synthesis and analysis. The government has for instance, already highlighted it’s concern with Deepseek.

A more robust framework may be required, not excluding the potential used of digital sanctioning.

3. Does the high-level Model resonate and do you have any suggestions for its refinement?

The high level model does resonate, particularly the “North Star” analogy for navigating the intent of the model, but there is a lot of complexity to it, which provides challenges in order to present this to community members, Executives and board members who are outside of the industry or industry-adjacent.

4. Can you suggest any existing or new ways to collect data and feedback to monitor these outcomes?

Quarterly engagement surveys administered by the Department of Home affairs, and a refresher / update on progress may assist. Communication of the findings from the surveys, segmented by Individuals, Practitioners, Government Organisations, and NFP may provide insights to proactively address outcomes not tracking to plan.

5. What could government do better to target and consolidate its cyber awareness message?

The Cyber awareness messaging is improving through official government channels, but it hasn’t really driven conversations at homes or at workplaces in the wider community.. It has been shared through various social media platforms. However, there may need to be a media activation such as out of home (Outdoor advertising)

Communication needs to achieve the right balance of ease of comprehension for non-technical members of the community, with potential links for substantiative technical analysis

8. How can industry at all levels and government work together to drive the uptake of cyber security actions by SMBs and the NFP sector to enhance our national cyber resilience? What type of support would be useful and who should provide it?

Participation and professional recognition of Industry advocates / a potential register for those who may be able to facilitate and also tailor domain specific communications relevant to the industry vertical

10.What are the unique challenges that NFP entities face for cyber security compared to the broader business sector and what interventions from government would have the most impact in the NFP sector?

Similar to the broader business sector, it's not typically the core activity of the entity to be involved in the development of Cyber Resilience Strategies.

However, as they draw on the use of volunteer labour who have already other commitments, it may not be front of mind what cyber security risks they may be exposed to, and the NFP may not have the same resources for threat-detection and response.

11.Do you consider cyber insurance products to be affordable and accessible, particularly for SMBs? If not, what factors are holding back uptake of cyber insurance?

There are levels of fragmentation in the Cyber Insurance product market, and there may be further work by the financial services industry to standardise the language between insured and uninsured events.

However, it is a positive step that there are providers who currently offer coverage for costs related to incident response, data forensic services, legal costs data breaches and business disruptions.

12.How well do you consider you understand the threat of ransomware, particularly for individuals and small entities? How is this threat evolving or changing?

Ransomware remains a current top cyber security risk for Individuals and Small entities.

Ransomware has evolved from initial malware like 'Cryptolocker' to many forks and imitations of similar functioning malware, which are not always detected through signature-based anti-malware software.

There are increasing levels of social engineering techniques to target individuals and small entities

However, it is proliferating from not just encrypting and preventing access to local and shared network drive files, to the take-down of websites, defacing them

15.How can support services for victims of identity crime be designed to be more effective in the context of increasing demand? How can technology be used to support individuals in managing and recovering from identity crime?

I am recommending that there is a national register that is developed and linked through the myGov website that draws on resources such as credit reporting services like

Equifax, Illion and similar that enable individuals to make assessments of when core identity documents are being by organisations.

It needs to be more straightforward, with potential 'push' notifications from the register, when certain events take place (e.g. Credit Application, New transactional account setup

20.What additional guidance do you or your organisation need to manage foreign ownership, control or influence risks associated with technology vendors?

There needs to be a clearer definition for industry, as to what sectors need to be 'on-shored' in terms of cloud data providers.

21.How could government better work with industry to understand data access and transfer across the economy to inform policies around secure data sharing and limit data exploitation from malicious actors?

The government can better assist industry, by potentially under the Office of the Information commissioner to be more prescriptive about data collection and retention periods.

Consumer Identity documents- retention 6 months

Customer

Medical information including Diagnostics

23.What guidance can government provide to support the safe and responsible uptake of critical and emerging technologies? What do you consider to be the most serious national security risks presented by critical and emerging technologies, such as AI?

Social engineering techniques will continue to grow, and are arguably becoming more believable with further advances in generative AI being used by nefarious actors.

Advances in compute processing ability may break early forms of encryption.

25.Does the government need to provide clarity on permissible and non-permissible Active Cyber Defence in the Australian context?

The government may be more explicit in terms of permissible and non-permissible defence mechanisms, including advice for organisations on 'Red-Team' penetration testing, and the responsibilities for individuals and businesses to conduct such testing.

26.How could government further support industry to block threats at scale?

There are still high levels of scam callers, I appreciate the observed recommendation for an business SMS register. But, high levels of scam calls are occurring from VOIP routed calls. There could potentially be a levy to increase the friction for VOIP registrants, and easier ways to report scam calls. Telecommunications providers should have an appropriate target and aggregate reporting for scam call volumes.

29.How can we better align and operationalise intelligence sharing for cyber security and scams prevention?

A quarterly cadence would assist with operationalising intelligence sharing with a case study, industry feedback, aggregate qualitive analysis and trends.

Recommend that for critical events, the communication that is shared by the National Cyber Security co-ordinator on an ad-hoc basis is useful.

30.Are the roles and responsibilities of government and industry clear for cyber security in a conflict or crisis scenario? What activities, such as cyber exercises, could Government undertake to make you feel better prepared to respond in a cyber conflict or crisis?

There are many government agencies with potential overlap, including State / Federal Police, the OIAC, ScamWatch, Home affairs, ASD and others.

This can create a bit of confusion within the community as the appropriate agency to contact, and potentially

39.What role should government play in supporting the development and growth of Australia's cyber workforce? What initiatives, pilots or policy ideas do you think would best support industry to grow?

42.How can industry, academia, think tanks and government best work together to set research priorities and drive innovation to further our strategic, economic and community interests and achieve our common goals?

I am currently conducting post graduate research into the area of Cyber Security risks at points of border crossing. I would be open to networking opportunities to advocate for the case further.

The Department of Home affairs, could provide further disclosure as to the priorities of certain initiatives after reviews of submissions are made within Horizon 2 with a cadence, and networking event.

Yours Sincerely,

[redacted]

[redacted]