15 April 2022

Ms Claire O'Neil, Minister; Australian Home Affairs,

Re: 2023-2030 Australian Cyber Security Strategy Discussion Paper Forum.

Public Submission

Dear Ms O'Neil,

I have followed with interest, and engagement the incoming government's commitment to Cyber Security, following comments made by Ed Husic MP that Labor was committed to the instatement of a dedicated cyber security minister, leading into the 2022 Federal election.

Following this commitment, and subsequent election, I note that you were appointed as the new Home Affairs and Cyber Security Minister.

I congratulate you for approaching your first 12 months within this portfolio.

During this time, there has been significant cyber security events that have gathered public and community attention, including the Optus, Medibank, and Latitude Financial data breaches.

I am a Data Analytics professional with over 20 years of developed Australian IT experience, across the areas of network administration, enterprise resource systems deployment and Business intelligence.

Simply put, I assist organisations in the deployment of reporting and analytical tools to assist with strategic decisions at scale, and finally scope appropriate develop associated security requirements.

I have an academic interest in Border Security, and recently completed a Graduate Certificate in Customs Administration.

I feel that there is an ongoing disconnect, across the public, the government, and businesses in terms of several areas.

As such, there needs to be a bi-partisan approach to address, objectively these issues as follows.

Personal and Private information:

There is a legitimate business and organisational need for Governments and NGOs to retain records on their customers; however, it should be clearly defined as to what information is classed as sensitive.

In particular, an extract from the Office of the Australian Information Commissioner (**OAIC**) is outlined below.

I. *'sensitive information' (includes information or opinion about an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation or criminal record, provided the information or opinion otherwise meets the definition of personal information)*
II. *'health information' (which is also 'sensitive information')*
III. *'credit information'*
IV. *'employee record' information*
V. *'tax file number information'.*

https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/what-is-personal-information#checklist-for-determining-whether-information-is-personal-information

The Cyber Security committee should work alongside the OAIC to make this more robust, with a Cyber security and data retention lens. There may be consideration for the draft of a Cyber Security Act to link specifically with what clause of the *Privacy Act 1988* (Cth).

Data Retention:

I would recommend that the committee considers and provides consultation as to what constitutes a current, or previous customer, in highly sensitive areas, such as Health, Financial Services, Energy & Telecommunications.

Restricting the access of Data retention, is in the public interest. Many of the customers impacted by Optus, Medibank and Latitude were seemingly surprised that their details were subject to the said attacks, as not having an active customer, or transactional history beyond this horizon. This would limit the potential size of 'Doxxing' attacks.

Consideration needs to be given, if beyond the statutory period of 5 Years, whether information is required to be retained in live production systems, or if such information can be decommissioned to alternative media or specialist providers of 'cold' data storage.

Data Access requests

Consumer Credit reporting agencies such as Equifax used by financial services often refer to State-Issued identification documents like Drivers License numbers, or Medicare numbers.

It may be useful for these access requests to be tracked, and logged independently by the government, and the subsequent enablement of public access.

In the case of Optus, and Medicare, there was limited information available to the public, as to the extent of the data breach, which customers may have been affected, and the last date of the access request.

Co-location and Data offshoring.

The majority of cloud-based software and solutions are now cloud and cross-regionally located. This can be for redundancy and availability purposes, coupled with practical considerations for speed and availability of data access for overseas-based support services for Australian businesses.

However, this can make the situation somewhat opaque for the public, as sensitive and personal information may be stored in overseas based data centres, without the appropriate due-diligence or security measures in place, as opposed to on-shore based services.

Such disclosures detailing where information is stored should be made transparently by organisations who capture sensitive information. Major platform providers such as Microsoft Azure, Amazon Web Services, and Google may be able to clearly differentiate product offerings to enable appropriate provisioning of co-location options.

Attack Sophistication:

The well-publicised attacks were classed as sophisticated, but in all fairness, they were achieved by poor internal corporate governance. In particular, Data Acquisition scripts which should have been stored within the organisations' private domain were uploaded to a community code-sourcing pages, GitHub & manipulated to perform external doxing attacks. In some instances, the motivations for such attacks, is not financially motived, however, it's to achieve notoriety within technical and hacking communities.

Social engineering forms of attacks, and including rudimentary impersonation of Australian based businesses are more prevalent. There should be a more co-ordinated response to reduce the increasing numbers of threats in these areas, such as the number of Linkt messages, and fake Australia Post SMS based attacks.

Complicated and organised attacks like Distributed Denial of Service attacks (Ddos) are unlikely, and improbable, but they should be considered for attacks on Critical infrastructure, such as Operational Technology. These have occurred overseas including the Oil India Attack, the Kudankulam Nuclear Power Plant Attack, and the Kemuri Water Company Attack.

Community Awareness

There should be consideration by the committee to help build some community awareness, in conjunction with the OAIC. Some practical examples include:

1. Importance of maintaining personal privacy for key government ID Documents:
   I. Driver Licence Numbers;
   II. Medicare Numbers;
   III. Passports; and
   IV. Birth Certificates.
2. The use of default passwords for off-the shelf home and business networking products.
3. How to detect a Fake SMS / Email or web address for impersonating an Australian business.
4. What applications have access to your sensitive information, including photos, files and location and how to check them?
5. How Single Sign On (SSO) works through Facebook, Google and Microsoft.

A suitable Television / outdoor advertising campaign may be a recommendation for the committee.

Don't let online Scammers steal your Identity!

This could also include references to self-help information available online.

Skills Shortage

There are further needs for the local training and development for information professionals, along with the building of awareness for public and private businesses. Suitable accredited training may be an opportunity for national harmonisation. Offensive and penetrative security testing capabilities would also be an ongoing requirement.

There is a recommendation that these capabilities are spread across a variety of providers, both large and small, to build resilience and diversity of capabilities.

Further investment in local cloud providers may also require suitably qualified staff. Partnerships with universities and state-based TAFE may be appropriate to deliver industry and vendor-based training opportunities.

In conclusion, the 2023-2030 Australian Cyber Security Strategy should encompass several key areas at a public policy level as the proposed Cyber Security Act requires consultation, and insight from the community practitioners and multiple government and non-government organisations.

I would welcome the opportunity to participate in the consultation process, in light of the above discussion areas.

Yours sincerely,

[redacted]