8 November 2019

Dear Hon Peter Dutton MP,

ANZ is pleased to provide its input into the development of the Australian 2020 Cyber Security Strategy.

I am personally happy to be contributing to the nation's second cyber security strategy, as one of the original authors of the 2016 Cyber Security Strategy. Transitioning from a career in government, to the position of Chief Information Security Officer for ANZ Bank, has not only enabled me to share this valuable experience within the private sector, it has also provided me with greater perspective on the full range of cyber security challenges facing organisations, including the massive growth of cybercrime.

Cyber security is recognised around the world as being a key priority for national and economic security, and as a key enabler of growth in the digital world. The Australian government must continue to play a critical role in working with business and academia to drive the national agenda to uplift and protect our people and our economy. It is not enough to deter and defeat cyber adversaries; this is an opportunity to innovate and thrive.

The key areas ANZ would like to see addressed in the next iteration of the Australian 2020 Cyber Security Strategy include:

1. Improved real time sharing of threat intelligence
2. More exercising to prepare for a major cyber incident
3. Improved utilisation of Joint Cyber Security Centres
4. Greater support for small-medium businesses, including a simple security standard
5. Continued support for education and a focus on improving awareness
6. Strong leadership from government on the importance of cyber security
7. Promotion of cyber security as a growth industry and enabler of economic growth
8. More work to help create a safer internet environment

We have seen good progress over the last three years, and have been proud to see the government and industry come together to deliver a number of great initiatives. However, we know these efforts need to be ramped up, and efficiencies found, in order to keep up with the growing pace, scale and sophistication of our adversaries.

[redacted]

Lynwen Connick

Chief Information Security Office
ANZ Banking Group

ANZ Security Domain
ANZ Centre, Level 9, 833 Collins Street
Docklands, Victoria 3008

Australia and New Zealand Banking Group Limited

1. Improved real time sharing of threat intelligence

While there has been some improvements in the sharing of threat intelligence, there is much room for improvement. For instance, ANZ receives far more information from the international Financial Services Information Sharing and Analysis Centre (FS-ISAC) than any Australian intelligence sharing arrangements.

But this is not just about sharing threat intelligence between the public and private sector. Many large corporations with significant cyber security capabilities generate their own threat intelligence, but sharing is ad hoc and largely based on trusted relationships. Government could play a greater role in facilitating threat intelligence sharing between and within industry sectors, in a manner that allows rapid ingestion and automated response, through the development of a secure threat intelligence sharing platform (perhaps learning from international examples such as the UK and EUROPOL).

2. More exercising to prepare for a major cyber incident

Critical services such as utilities, telecommunications, transport, healthcare, emergency services, and financial services underpin the operations of Australian business and its citizens. This also makes them an attractive target for cyber-attacks.

Around the world, we are increasingly seeing cyber-attacks on critical infrastructure, and offensive cyber capabilities being used as a tool of state. While many industry sectors exercise their incident response capabilities, a major cyber event is likely to have a wide range of impacts, and will require a highly coordinated response. Exercising and testing this on a regular basis is critical if we are to respond effectively in the event of an actual attack.

Government should take the lead in coordinating national cross-sector cyber security exercises involving government, business and industry regulators using defined threat scenarios.

3. Improved utilisation of the Joint Cyber Security Centres

The 2016 strategy delivered Joint Cyber Security Centres (JCSCs) in Sydney, Melbourne, Brisbane, Adelaide and Perth. While the new facilities are now fully established, their effectiveness as a regional hub for cyber security collaboration is yet to be fully realised. We would like to see a clearer role for the centres as a regional arm of the Australian Cyber Security Centre, which may entail establishing a greater level of local technical expertise.

This could include activities such as greater use of JCSCs as the coordination centre for incident response, industry workshops to identify common community objectives and challenges with security professionals, more small business education and training events, as well as community advisory groups.

4. Greater support for small-medium businesses, including a simple security standard for all businesses

Outside large corporations like ANZ, most Australian businesses businesses are ill-equipped to defend against, and respond to a cyber-attack. Most do not have their own cyber security capabilities and are therefore reliant on service providers, whose service offerings and quality can vary widely. Furthermore, many business do not have the requisite technical knowledge to understand their security requirements or assess the ability of service providers to meet them.

We do not believe that more regulation is required, but we do think a simple voluntary security standard – perhaps drawing on established models such as the ASD Essential 8 – would help provide businesses with a level of assurance that their most critical security needs are being met. This is also important for financial organisations operating under APRA's new CPS 234 Information Security Standard, which requires service providers and other third parties to demonstrate they have an appropriate level of information security capability. A common standard would minimise the need for multiple supplier assessments.

In addition to the standard, we see real benefit in the provision of simple and reliable information and tools to assist small business in this area, including things like risk assessment templates, checklists, "how to" advice and listings of reliable organisations to perform information security assessments.

Finally, given the increasing levels of cybercrime, we would like to see simplified reporting arrangements and standard processes for dealing with victims of computer-based crime.

5. Continued support for improved security awareness and education

Cyber security can be complex and confusing for many people, particularly vulnerable groups such as the elderly and people from non-English speaking backgrounds. To build a cyber smart nation we need to ensure that everyone is able to seize the opportunities offered by digital technologies, safely and securely. The strategy must address how we involve every person and organisation in taking action, to learn about, and adopt digital technologies safely.

Beyond this, every job of the future will evolve with technological change and require a higher level of digital literacy. We need to continue to incorporate information security into all levels of education, both to raise the general level of security awareness, and to foster a ready pool of skilled information technology and cyber security manpower, to help companies and the Government seize technological opportunities as and when they arise.

Initiatives which could contribute to these objectives include:

- Providing more general security information from the Australian Cyber Security Centre, on the cyber.gov.au webpages and social media, similar to the content from the National Cyber Security Centre in the UK.
- Creating a national cyber safety and awareness curriculum that is taught in secondary and primary schools consistently across the country**.**
- Investing in supporting, upskilling and training teachers in IT and security, to ensure educators in schools and universities keep up with the latest technology and cyber security developments.
- Creating more apprenticeships and pathways that are a combination of TAFE and workplace employment.
- Encouraging a Framework of cyber security roles in Australia similar to the National Initiative for Cybersecurity Education (NICE) framework in the US.
- Retraining and increasing our pool of qualified professionals, looking into other areas to increase the diversity of our workforce.

6. Strong leadership from Government

The 2016 strategy has established the foundations of a national cyber partnership between government, business and academia. The new strategy needs to build on this, by capitalising on the learnings and experience of leaders across these areas, while continuing to provide clear and tangible goals and objectives to enhance Australia's cyber security posture, at all levels.

Increasing cross-sector working groups to collaborate on our biggest issues will benefit from greater diversity of knowledge, efficiencies and stronger networks. This could include coordinating activities such as heads of industry think tanks to address critical economic and business issues relating to cyber security, innovation sessions to identify new and proactive opportunities and industry sector working groups to tackle common issues.

7. Promote cyber security as a growth industry and enabler of economic growth

Disruptive technologies will open up new business opportunities, but many of these depend on trust and confidence in the security of cyberspace. Getting 'cyber security right' will mean Australia is a secure and dynamic location for business diversification and investment.

While Australia's cyber security sector remains small, it has a strong international reputation and is forecast to grow due to increased demand for cyber security products and services. The establishment of AustCyber is already having a significant impact, and the new strategy needs to continue to promote measures which create the right environment to incubate cyber security research, development and start-ups.

8. More work to help create a safer internet environment

The strategy should clearly identify measures which could be put in place to help create a safer internet environment for all Australians utilising the capabilities of government and industry. For instance, telecommunications companies and large internet service providers should proactively filter and block known malicious activity at a national level (similar to the way that banks monitor, detect and shut down fraudulent card activity).

Similarly, government should play a greater role, using some of its unique authorities and capabilities, to actively shut down known bad actors such as botnets and hoax/scam websites. Government should also take a leading role in the development of a national digital identity framework to facilitate better and more secure ways to authenticate.