CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

Cyber Security Research Centre Limited
ABN 11 605 454 144

Australia's 2020 Cyber Security Strategy: Submission from the Cyber Security Cooperative Research Centre (Cyber Security CRC)

CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

13 November 2019

Dear Sir/Madam

Response to the 'Call for Views' – Australia's 2020 Cyber Security Strategy

I am pleased to submit the Cyber Security Cooperative Research Centre's ('CSCRC') response to the call for views on Australia's 2020 Cyber Security Strategy (the Discussion Paper). Government is to be commended for the progress to date from the 2016 Cyber Security Strategy. The 2020 Cyber Security Strategy 'Call for Views' demonstrates there is still much work to be done.

About the Cyber Security Cooperative Research Centre

The CSCRC was formally established in 2018 following the 2016 Cyber Security Strategy. The CSCRC is dedicated to developing innovative projects that strengthen Australia's cyber security capabilities and that deliver outstanding cyber security research that creates commercial solutions to pressing problems.

The CSCRC is a public company limited by guarantee and it will invest $AU50 million of Australian Commonwealth Government funding, and additional Participant funding over seven years to 2025 in research outcomes related to our key impact areas.

CSCRC aims:

- to be a leading provider of cyber security research with impact in Australia that enables innovative approaches, tools and advice;
- to build national and international confidence in Australia being a safe and trusted place to do business;
- to build and develop the next generation of cyber security leaders; and
- to contribute to the public good and produce R&D activities in a challenging and fast-moving environment.

The CSCRC has 24 Participants including 7 Research Providers, 7 State and Federal Government Agencies/Departments - including the Australian Signals Directorate (ASD) - and 10 Industry/SMEs. The CSCRC has 3 research programs: Critical Infrastructure Security, Cyber Security as a Service, and Law and Policy. As of November 2019, the CSCRC had 45 ongoing or concluded projects.

This submission is very broad based. We look forward to answering any queries about this submission and welcome the opportunity to participate in future discussions on Australia's 2020 Cyber Security Strategy.

Yours Sincerely,

[redacted]

Rachael Falk
CEO
Cyber Security Cooperative Research Centre
[redacted]

Executive Summary

The Australian Government's '2020 Cyber Security Strategy Discussion Paper' (the Discussion Paper) outlines progress to date on the Government's 2016 Cyber Security Strategy, and highlights areas where the Government is seeking advice and guidance for the 2020 Strategy across five key sections:

1. Government's role in a changing world;
2. Enterprise, innovation, and cyber security;
3. A trusted marketplace with skilled professionals;
4. A hostile environment for malicious cyber actors; and
5. A cyber-aware community.

The CSCRC has aligned its submission with these sections – with specific focus on sections 1, 2, 3 and 5.

There is no doubt that the challenges as set out in the 26 questions in the Discussion Paper are complex and not unique to Australia. There are areas, however, where Australia could be a world leader in addressing the opportunities and challenges inherent in cyber security.

One example of possible global leadership could be in enshrining a National Data Policy together with minimum cyber security standards in legislation with real consequences for organisations and recognition of harm for victims. Another example is Australia's continued commitment to ensuring that crimes that are inspired and facilitated online are recognised as offences just as they would be in the 'real world'.

The CSCRC makes the following key observations and recommendations for the Government's 2020 revised cyber security strategy:

- That there be ongoing commitment of resources to ensure that Australia remains a trusted and safe place to do business and engage online;
- That there be greater support for the principle that there should be no difference between the online or offline environment when it comes to rule of law and recognition of criminal activity;
- That public trust be further enhanced though the ongoing recognition of the interdependent roles and responsibilities of Government, industry and the community;
- That the role of Small Business Cyber Security Advisor be created to lead the way in advising on effective cyber security mitigation strategies (that result in actual security uplift) for small to medium businesses along with targeted programs that build resilience for this vitally important part of the business community. This senior role should be the face of cyber security for small to medium enterprises;
- That a revised legal framework where Australia can lead the way in setting minimum cyber security standards for Listed Companies be developed and enshrined in legislation;
- That there be further consideration of regulatory reforms, starting with the recommendations made by the Australian Competition and Consumer Commission's (ACCC) Digital Platforms Inquiry;
- That there be continued support from Government for the development of Australia's sovereign cyber security capabilities;
- That there be a continued commitment from Government to work with industry and academia on supporting cyber security innovation through research and building sovereign capability via scholarships and other programs. The creation of the CSCRC and AustCyber are examples of such commitment by Government; and
- That consideration be given to establishing a National Data Policy which sets national standards (and accreditation) for the protected storage, transmission and use of sensitive Australian citizen data collected by Government and industry.

CYBER SECURITY COOPERATIVE RESEARCH CENTRE

1) Government's role in a changing world

1. *What is your view of the cyber threat environment? What threats should Government be focusing on?*
2. *Do you agree with our understanding of who is responsible for managing cyber risks in the economy?*
3. *Do you think the way these responsibilities are currently allocated is right? What changes should we consider?*
4. *What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?*
5. *How can Government maintain trust from the Australian community when using its cyber security capabilities?*

Australians live in an increasingly connected world. In 2018 the average Australian household had 17.1 connected devices, which is expected to grow to 30 by 2021.[1] The rapid approach of 5G technology will enable greater speeds, access to data, more automation and device connectivity. The Internet of Things (IoT) is estimated to achieve potential annual benefits of between $194-308 billion over a period of 8-18 years across a range of industries.[2]

However, living in a connected world brings both risks and unintended consequences that need to be effectively managed. Protecting systems and data from cyber disruption and attack will become more complex and challenging, especially as supply chains are globalised.

The 2016 Australian Cyber Security Strategy recognised the need for whole-of-society action. One of the recommended measures in the 'Cyber Smart Nation' theme was the establishment of the Cyber Security Cooperative Research Centre (CSCRC) that harnessed the strengths of industry, academia and Government to focus Australia's world-leading research capabilities on solving today's and tomorrow's cyber security challenges. [3]

We recognise the environment has changed since the release of the 2016 Strategy – the challenges have evolved. Cyber security has moved from being a niche or technical issue as more people live their lives in an increasingly connected world.

In October 2019 the Australian Cyber Security Centre (ACSC) reported that Australians made 13,500 reports of cyber-crime between 1 July and 30 September 2019 – about 1 report every 10 minutes.[4] Over 6 million – or 1 in 4 – Australian adults were impacted by cybercrime in 2017.[5] According to the Cisco 2019 APAC CISO Benchmark study, cyber security incidents have had a higher cost in Australia than in other Asia-Pacific countries, with 84% of surveyed organisations in Australia suffering a breach in 2019 that cost them over $1 million.[6] The same report also found that in 2019 Australian corporations received twice the amount of daily security alerts than they did in 2018 – meanwhile, the percentage of real security incidents that have been fixed has dropped by 31%.[7]

[1] 'On track for over 30 connected devices per Aussie household by 2021,' *NBN Blog,* 29 May 2019 https://www.nbnco.com.au/blog/connected-homes/on-track-for-over-30-iot-devices-per-aussie-household-by-2021
[2] PwC, 'Australia's IoT Opportunity: Driving Future Growth', *Australia Computer Society,* September 2018 https://www.acs.org.au/content/dam/acs/acs-publications/ACS-PwC-IoT-report-web.pdf
[3] See 'Australian Cyber Security Strategy', p 52 ('Cyber Security Research Centre' was formerly known as 'Australian Cyber Security Research Institute')
[4] Stephanie Borys, 'You could soon be a victim of cybercrime — here's how to try to stop that happening', *ABC News,* 8 October 2019 https://www.abc.net.au/news/2019-10-07/cyber-crime-how-to-help-protect-yourself/11577930
[5] 'Stay Smart Online Week 2018', *Australian cyber Security Centre,* 2018 https://www.staysmartonline.gov.au/get-involved/see-it-action/stay-smart-online-week-2018
[6] Cisco, *Anticipating the Unknowns: 2019 Asia Pacific CISO Benchmark Study*, 2019 October, p 18.
[7] Cisco, *Anticipating the Unknowns*, p 18.

It is a legitimate role of Government to address this global challenge through providing leadership and collaboration with industry and the research community.

While individuals can take steps to protect themselves, Government and industry have a responsibility to effectively manage cyber risk. Sensitive data on Australian citizens whether it is held by Government, industry or academia should be held in accordance with minimum cyber security standards alongside a National Data Policy.

The Government has a clear role in designing legislation to raise the bar for organisations on good cyber security practice so that valuable sensitive data is protected in line with such legislation. This could be a useful way to improve baseline cyber security capabilities. There should also be significant consequences if minimum standards are not met or there is flagrant disregard for how organisations treat customer and sensitive data.

Trust between Government, industry and the Australian community is essential to Australia's digital security. Public trust can be further enhanced though the ongoing recognition of the interdependent roles and responsibilities of Government, industry and the community.

It is vitally important for Government to continue its existing narrative around legal principles applying both online and offline. What is illegal in the offline world must be illegal in the online world. Law enforcement and intelligence agencies must have the tools and appropriate processes to operate in a challenging threat environment and to prevent and prosecute such crimes. Legislation such as the *Telecommunications and Other Legislative Amendments ('Assistance and Access') Act 2018* and the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* are appropriate responses to an environment where organised crime, terrorism, and fraud is frequently amplified, inspired and facilitated online.

Government contributes to public trust when it confirms its role (where it will and will not assist industry) and where it is clear about what private individuals and organisations should not be doing when it comes to responding to cyber-attacks.

Organisations or individuals at the receiving end of cyber-attacks, for example, should not attempt to play 'digital vigilante'. Internal CSCRC research has found that organisations attempting to 'hack back' against cyber criminals or nation states are likely to be engaging in unlawful conduct, are unlikely to 'catch' the real criminal, are unlikely to recover their data and they might cause serious unintended consequences. Boards and management have a responsibility to familiarise themselves with their organisation's cyber risk. Government should make clear that all cyber-attacks should be reported to the Australian Cyber Security Centre (ACSC) and continue to offer clear guidance and assistance where it makes sense for them to do so. To be clear, in our view, it is not the role of Government or the ACSC to step in and remediate a cyber-attack nor is it the role of Government or the ACSC to provide resources when an organisation has failed to implement adequate mitigation strategies.

The ACSC plays (and should continue to play) a particularly important role in promoting cyber resilience across the whole of the economy, including critical infrastructure, all levels of Government, small to medium business, academia, the not-for-profit sector and finally the Australian community.

There could be merit in situating within the ACSC a new senior role of Small Business Cyber Security Advisor to lead the way in advising on effective cyber security mitigation strategies (that result in actual security uplift) for small to medium businesses. The Small Business Cyber Security Advisor could also have oversight of targeted programs that build resilience for this vitally important part of the business community.

Finally, Government has a continuing role in supporting industry-led research and development so that Australia can continue to play a significant role in innovation and collaboration in cyber security. The CRC Program is a tried and tested mechanism for facilitating research collaboration. The Program has been repeatedly reviewed and each time it has proven that it provides the Australian taxpayer value for money and significantly adds to Australian innovation.

2) Enterprise, innovation, and cyber security

6. *What customer protections should apply to the security of cyber goods and services?*
7. *What role can Government and industry play in supporting the cyber security of consumers?*
8. *How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?*
9. *Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?*
10. *Is the regulatory environment for cyber security appropriate? Why or why not?*
11. *What specific market incentives or regulatory changes should Government consider?*

Minimum cyber security standards for organisations

It is important to recognise that industry (particularly large organisations) derive significant benefit from use of their customers' data. It should further be recognised that those organisations that derive benefit must also ensure that they effectively manage the risk of storing, using, and sharing such valuable data. There is an opportunity for legislative intervention to ensure that there is adequate protection of this valuable data.

Australia can be a leader and demonstrate its commitment to making Australia a safe and trusted place to do business for all. An opportunity exists to create minimum cyber security standards (enshrined in legislation) that include ASD's Essential Eight (or similar) as well as other conditions by which sensitive data is managed. To ensure that these standards result in a security uplift in organisations, they could be coupled with consequences, such as a breach of these standards being a strict liability offence. This would mean that if an organisation has a data breach and their customers suffer damage as a result of that breach, those customers would not have to go through significant legal hoops to obtain some damages.

At present Australian common law does not recognise cyber harms as an injury that results in actual loss. The more recent amendments to *Privacy Act* Cth (1988) recognise such harms but it is submitted that these changes have not resulted in any investigations or payments to victims of breaches. It is not clear why the current regulator, the Office of the Australian Information Commissioner (OAIC), has not used its power to signal the market. This is an opportunity for Australia to lead the way in enshrining recognition of cyber harms in legislation with minimum standards and real consequences for industry when these breaches occur.

The ACCC's Digital Platforms Inquiry demonstrated that the legal settings around privacy in Australia are not in line with international standards and consumer interests, and that more must be done to strengthen Australia's privacy protections.[8] Many privacy policies are "misnomers", outlining the ways an organisation may use consumer data rather than how they will protect privacy.[9]

There is a need for regulatory reform to better protect consumers. This could be considered by a mechanism such as a working group, alongside other regulatory reforms such as those proposed by the Australia Law Reform Council in their report '*Serious Invasions of Privacy in the Digital Era'*. A mechanism for examining regulatory reforms should seek to balance openness, transparency and innovation with privacy, security, and competition.

Further, there could be merit in establishing a National Data Policy which sets national standards (and accreditation) for the protected storage, transmission and use of sensitive Australian citizen data collected by Government and industry.

[8] Rachael Falk, 'Data gluttony in business raises need for privacy reform,' *Australian Financial Review,* 5 August 2019 https://www.afr.com/technology/data-gluttony-in-businesses-raises-need-for-privacy-reform-20190801-p52cqy
[9] Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Final Report,* 2018, p 383

Regulation of technology platforms

Technology platforms ought to be subject to appropriately similar obligations to institutions that operate in the physical world. The Discussion Paper outlines Europe's Network and Information Security (NIS) Directive as a case study for regulation. Critical infrastructure in Australia is already regulated, covering aspects of cyber security. However, the advantage of Directives such as NIS, is that it establishes a common reference framework to ease communication and collaboration between countries. We believe that this is a significant advantage for the protection of critical infrastructures that cross state boundaries. It also supports operations and compliance assessments for organisations that operate across state and country boundaries.

Cyber security is far more than just a technical field. Law and policy have an essential role in ensuring that online behaviour is consistent with the public's expectations about their privacy and security. Organisational culture and attitudes about cyber security is one of the top 3 obstacles for organisations looking to improve their cyber security posture.[10] Though the majority of executive leaders see cyber security as a high priority, 19% of organisations' leaders do not, which is higher than both the regional and global average.[11]

3) A trusted marketplace with skilled professionals

One of the CSCRC's core missions is to build the cyber security professionals of tomorrow. We acknowledge that while the CSCRC's focus is supporting outstanding academics and students by providing them with scholarships to work on CSCRC research projects, there is a need to ensure that there should be minimum standards for some cyber security professionals. However, we would submit that industry is best placed to articulate what they need and what those requirements should be.

AustCyber estimates that Australia will face a shortfall of 18,000 cyber security professionals over the next seven years.[12] Cisco has found that 22% of Australian organisations lack trained cyber security personnel, and 21% lacked knowledge about advanced security processes and technology.[13] The Australian Government's commitment to the CSCRC, which plays an important role in cyber security education and training, recognised the need to equip the nation with skilled cyber security professionals as well as a cyber-literate workforce.

Nonetheless, CSCRC submits that advances in machine learning and artificial intelligence (AI) are likely to automate many of the basic cyber security requirements currently met by trained personnel – this needs to be taken into account in terms of long term planning for both academic programs and the types of workforce Australia will need in the next 10-15 years.

The need for advanced cyber security products and services – a sector that is projected to be worth US$248 billion globally by 2026[14] – will not be met by training people only in basic network security. Skillsets need to be diverse and include skills such as critical thinking and ethics to enable digital products to be secure-by-design and to operate as intended. Similarly, cyber security professionals of the future will need to have legal, regulatory, marketing and other qualifications. Any long-term planning with respect to building skilled professionals must include a broad approach and not just be confined to STEM-based qualifications.

[10] Cisco, *Anticipating the Unknowns*, p 19.
[11] Cisco, *Anticipating the Unknowns,* p 19.
[12] 'Educate', *AustCyber* https://www.austcyber.com/educate
[13] Ibid, 19.
[14] 'SCP - Chapter 1 - The global outlook for cyber security', *AustCyber Sector Competitiveness Plan 2018,* https://www.austcyber.com/resources/sector-competitiveness-plan/chapter1

CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

4) A cyber-aware community

In the 2017 ASX Cyber Health Check Report only 45% of companies (who responded to the survey) identified as being very confident or confident in their organisation's ability to detect, respond to and manage a cyber intrusion. That statistic suggests that most companies are feeling overwhelmed and under prepared.

Corporate boards must engage with cyber risk and regard it as just another business risk[15]. But with multiple institutions promoting different messages, cyber security can seem overwhelming or too difficult, especially since it is already regarded as a 'tech problem'. Similarly, it can be challenging for boards to assess what 'good' looks like when it comes to mitigating cyber security risk.

It is clear that there is still an overwhelming need to ensure that everyone from the boardroom down understands the risks that come with living in a connected world. A targeted and regular national campaign for all Australians about the importance of protecting valuable data, limiting who has access to that data, and deciding when and how it should be shared is critical.

The Small Business Cyber Security Advisor proposed earlier would also contribute to a building more cyber-aware community.

November 2019

[15] Rachael Falk, 'It's time to reboot Australia's cybersecurity strategy' *ASPI*, 4 October 2019 https://www.aspistrategist.org.au/its-time-to-reboot-australias-cybersecurity-strategy/