AUSTRALIA'S 2020 CYBER SECURITY STRATEGY

A Call for Views

Department of Home Affairs

Australian Government

SUBMISSION

Submitted by

Organisation: (ISC)²

Lead Author: Tony Vizza

Director for Cyber Security Advocacy

Asia-Pacific

Email: [redacted]

Phone: [redacted]

Postcode: 2000

Category: Other – (ISC)² – Information Security Industry Body – Not for Profit

Consent: This submission can be published.

EXECUTIVE SUMMARY

(ISC)² welcomes the Australian Government's Call for Views in relation to Australia's 2020 Cyber Security Strategy.

(ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, programmatic approach to security. Our membership, more than 140,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the public through our charitable foundation – The Center for Cyber Safety and Education™.

(ISC)²'s mission is to support and provide members and constituents with credentials, resources and leadership to address cyber, information, software and infrastructure security to deliver value to society**.** The association was the first information security certifying body to meet the requirements of ANSI/ISO/IEC Standard 17024, a global benchmark for personnel certification. All (ISC)² certifications have been accredited against this standard, making (ISC)² credentials a must-have among professionals and employers.

In Australia, (ISC)² has formed strong, strategic partnerships with the Australian Cyber Security Centre (ACSC), Australian Information Security Association (AISA) and the Australian Computer Society (ACS). In addition to this, partnerships have been formed with the Government of Victoria and Government of NSW, as well as working relationships with other state governments. (ISC)² also works collaboratively with AustCyber, the Office of the e-Safety Commissioner, universities across Australia as well as industry bodies including the Australian Security Industry Association (ASIAL), the IoT Alliance of Australia, the Financial Services Council and Blockchain Australia.

Around the world, (ISC)² has formed strong and long-lasting partnerships with the National Institute of Standards and Technology (NIST) and National Institute for Cybersecurity Education (NICE) in the US, ANSI/ISO/IEC globally and works closely with government agencies and bodies in the Five Eves group of nations, across the Asia-Pacific region and around the world. As a result of the leadership position (ISC)² has taken to promote a safer and more secure cyber world, (ISC)² credentials are considered to be the gold standard in cyber security certification and excellence around the world.

The response offered by (ISC)² represents the collective views of over 145,000 certified cyber security professionals globally. These professionals are tasked with protecting and securing public and private sector organisations including national, state and regional governments, Fortune 100 companies, large enterprise, NGO's as well as SME/SMB across all industries, verticals and sectors.

It is hoped that the Federal Government will consider these views and incorporate the recommendations as part of the future cyber security strategy of Australia to help deliver Australians a safer and more secure cyber world, both now and well into the future.

TABLE OF CONTENTS

FORMAL RESPONSES

QUESTION 1 – WHAT IS YOUR VIEW OF THE CYBER THREAT ENVIRONMENT? WHAT THREATS SHOULD GOVERNMENT BE FOCUSING ON?

The current cyber threat environment is well documented. The Call for Views includes empirical data on the threat environment from a number of reputable sources, which succinctly illustrates the gravity and severity of the situation as it currently stands.

Of greater concern is the view of the cyber threat environment in the foreseeable future. With the continuing development of digitization, interconnectedness, the ubiquity of social media platforms, the age of the Internet of Things (IoT) and the erosion of the concept of privacy, there is significant risk that the current cyber threat environment will only escalate. This view is reinforced by research from organisations such as the World Economic Forum that regard cyber security and privacy-related risks as two of the top five global risks in terms of likelihood.[1]

Much of this risk can be attributable to the human element within cyber security, with the OAIC reports indicating that at least 67% of breaches in Australia are caused by human error.[2] Given that humans are exposed to information technology from a very young age and research indicates that 90% of two-year old children had proficiency in using an electronic smart tablet,[3] it is incumbent on government to consider the societal risks associated with cybers security.

In addition to cyber related threats, competitive threats also exist for Australia on the world stage. With the cyber security skills shortage well documented both by international organisations such as (ISC)[2] in its annual Cybersecurity Workforce Study[4] as well as Australian government entities such as AustCyber[5], addressing the skills gap to ensure that the Australian economy both trains and retains quality cyber security talent is essential to meeting the challenge of remaining competitive on the world stage.

As the world's largest association of certified cyber security professionals, (ISC)[2] contends that the single biggest area for focus by government, both in Australia as well as globally, should be in the cyber security education area. Measures that can be adopted by the Federal Government to meet these challenges include but are not limited to:

- Ensuring cyber security professionals are duly certified in globally recognised certifications to perform their duties and responsibilities in line with industry best practice and ensure their organisations are adequately protected.
- Ensuring adequate investment in cyber education from a young age, including at pre-school level and continuing through primary and secondary school, to ensure that toddlers, children and teenagers understand the cyber threats applicable to them as they grow up and as the social environments they belong to evolve.
- Ensuring vocational education providers such as TAFE's and private sector providers align their cyber security course curricula to global industry standards such as those provided in the U.S. Government's NICE (National Institute for Cybersecurity Education) framework.
- Ensuring Australia's universities align their cyber security programs to global industry standards and partner with global peak industry bodies such as (ISC)[2] to ensure that graduates possess both the appropriate skills as well as prudent mindset required to be effective cyber security professionals.

[1] World Economic Forum, 'Global Risk Report 2019', http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.
[2] Australian Computer Society, 'Human error the leading cause of data breaches', https://ia.acs.org.au/article/2019/human-error-a-leading-cause-of-data-breaches.html
[3] Juan Pablo Hourcade et al, University of Iowa, 'Look, My Baby is using an iPad! An analysis of YouTube videos of infants and toddlers using tablets', https://dl.acm.org/citation.cfm?doid=2702123.2702266, 2015.
[4] (ISC)[2], 'Cybersecurity Workforce Study, 2019', https://www.isc2.org/Research/Workforce-Study
[5] AustCyber, 'SCP – Chapter 3 – The Challenge: Australia needs to fill the workforce gap, remove startup barriers and strengthen research and development', https://www.austcyber.com/resources/sector-competitiveness-plan/chapter3

QUESTION 6 – WHAT CONSUMER PROTECTIONS SHOULD APPLY TO THE SECURITY OF CYBER GOODS AND SERVICES?

The role of government to regulate products and services across Australia at a national level is well established. Given the increasing prevalence of technological products and services dependent on this technology, it is the view of (ISC)[2] that the Australian government should consider regulations to ensure safe and secure outcomes for consumers. In addition, (ISC)[2] considers that the role of government in protecting the privacy of its citizens is essential and serves as a fundamental and implied obligation of government in any advanced democracy such as Australia.

There are three main areas that (ISC)[2] considers that the Federal Government can focus on to affect positive change:

1. The adoption of regulations to ensure that manufacturers of information technology products incorporate best practice cyber security protections within the products they manufacture to ensure they meet a minimum level of protection for consumers. The state legislature of California in the United States recently passed Senate Bill No. 327[6] to offer consumers appropriate levels of protection, and the Federal Government should consider similar regulation to ensure products are fit for sale.

2. The adoption of a licencing or recognition scheme for information technology and cyber security services providers to ensure that consumers make informed decisions about the provider they choose to engage with. The environment in which information technology and cyber security services providers lacks any form of licencing or regulation, and any person, whether they are trained, qualified, certified or not, is able to establish and operate a business in the industry. While the Australian Signals Directorate has created the IRAP Assessor program[7], this program is designed for Government use. The proposed licencing or recognition scheme should be based on an organisation's attainment of a minimum level of technical proficiency which should include:

    a. Attainment by organisations of the internationally accepted ISO/IEC 27001:2018 information security management accreditation[8] to demonstrate that the organisation is capable of protecting the information security assets of both its own operations, as well as of its customers.

    b. Employment of cyber security personnel in key areas of responsibility who are duly accredited and certified by an ANSI/ISO/IEC 17024 accredited global peak industry body such (ISC)[2] in certifications that align to the US Governments NICE (National Institute of Cybersecurity Education) Cyber Security Workforce Framework.

3. Modernisation of the Commonwealth ***Privacy Act 1988*** to ensure that the privacy needs of individuals and businesses are met in today's digital era. There is an increasing view that privacy is being eroded due to the monetisation of data by "big tech" and many jurisdictions around the world have either strengthened or are considering strengthening privacy rules to ensure that citizens are able to use technology and exercising a level of privacy that they deem acceptable. An appropriate scheme to consider by the Federal Government to achieve this would be one that is based on the European Union's General Data Protection Regulation (GDPR).[9]

[6] ***Senate Bill No. 327 Information Privacy: Connected Devices*** (California), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.
[7] Australian Signals Directorate, Australian Government, 'What is IRAP?', https://www.cyber.gov.au/irap/what-irap.
[8] Organisation Internationale de Normalisation (ISO), 'ISO/ISC 27001 Information Security Management', https://www.iso.org/isoiec-27001-information-security.html.
[9] European Commission, 'EU data protection rules', https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

QUESTION 14 – HOW CAN AUSTRALIAN GOVERNMENTS AND PRIVATE ENTITIES BUILD A MARKET OF HIGH-QUALITY CYBER SECURITY PROFESSIONALS IN AUSTRALIA?

The cyber security skills shortage both in Australia and around the world is well documented. Estimates of the cyber skills gap range from:

- (ISC)[2] research indicating there is a global shortfall of 4.07 million cyber security professionals in the world and 45,000 workers in Australia today.[10]
- AustCyber estimating an existing shortfall of 2,300 cyber security workers today with an additional 17,600 cyber security workers required by 2026.[11]
- The Australian Computer Society (ACS) estimating that Australia will require an additional 100,000 information technology workers by 2024, with many of these roles in cyber security.[12]
- Job site Indeed claiming that Australia has only 7% of the cyber security expertise needed to meet current demand.[13]
- Recruiting firm Hays indicating that 61% of business leaders claim it is "difficult or very difficult" to recruit cyber security talent.[14]

With Federal Government departments such as the Australian Federal Police (AFP) decrying the lack of available cyber security talent and its inability to retain cyber security professionals,[15] there is a clear, present and desperate requirement for government to address the skills gap that exists and to build a strong and capable market of cyber security professionals.

There are a number of broad areas that Government, both Federal and State, can address to build a pipeline of high-quality cyber security professionals in Australia. These measures include:

- Adopting the highly-regarded US Government NICE Framework[16] which serves as a reference structure describing the interdisciplinary nature of the work involved in cyber security.
- Developing domestic capacity to establish an environment where a career in cyber security will appeal to a wider and more diverse group of both able and disabled men and women, as well as diversity in skill sets that includes both technical and non-technical personnel.
- Supporting Australians seeking a career in cyber security by ensuring tertiary education providers teach relevant, cost-effective and industry-leading skills and ensuring the programs incorporate an experiential element to help students build practical experience to supplement the knowledge gained from the program.
- Supporting Australian organisations seeking to employ new entrants into the cyber security field with access to training, education, skills and experience through the provision of grants tied to enrolment in programs accredited by Government including Universities, TAFE's and private sector organisations teaching industry accredited programs.
- Working with ANSI/ISO/IEC 17024[17] accredited global cyber security peak bodies such as (ISC)[2] to ensure that cyber security professionals are certified to an ANSI/ISO/IEC accredited personnel certification standard.
- Introducing a positive concept of cyber security within the school environment and incorporating cyber security skills into the school curriculum in order for school students and leavers to consider a career in cyber security.

---

[10] (ISC)[2], 'Cybersecurity Workforce Study, 2019', https://www.isc2.org/Research/Workforce-Study

[11] AustCyber, 'SCP – Chapter 3 – The Challenge: Australia needs to fill the workforce gap, remove start-up barriers and strengthen research and development', https://www.austcyber.com/resources/sector-competitiveness-plan/chapter3.

[12] Australian Computer Society, 'ACS Australia's Digital Pulse 2019', https://www.acs.org.au/insightsandpublications/reports-publications/digital-pulse-2019.html

[13] CSO.com.au, 'Australia only has 7 percent of the cybersecurity expertise that it needs', https://www.cso.com.au/article/645445/australia-only-has-7-percent-cybersecurity-expertise-it-needs/, 20th August 2018.

[14] ITwire.com.au, 'Cyber security 'talent gap' hinders recruitment: report', https://www.itwire.com/security/cyber-security-%E2%80%98talent-gap%E2%80%99-hinders-recruitment-report.html, 2nd July 2019.

[15] ITnews.com.au, AFP copping cyber skills shortage hard warns chief', https://www.itnews.com.au/news/afp-copping-cyber-skills-shortage-hard-warns-chief-519687, 25th February 2019.

[16] National Initiative for Cybersecurity Education (NICE), U.S. Department of Commerce, United States Government, 'NIST Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework', https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

[17] Organisation Internationale de Normalisation (ISO), 'ISO/IEC 17024:2012 Conformity assessment — General requirements for bodies operating certification of persons', https://www.iso.org/standard/52993.html.