Submission No 20

INQUIRY INTO CYBERSECURITY

Organisation: (ISC)2

Date Received: 19 September 2020

Inquiry into Cybersecurity

Legislative Council
Parliament of New South Wales

SUBMISSION

Submitted by

Organisation: (ISC)^2
Lead Author: Tony Vizza, Director for Cyber Security Advocacy, Asia-Pacific

Postcode: 2000
Category: Other – (ISC)^2 – Information Security Industry Body – Not for Profit
Consent: This submission can be made public and published.

EXECUTIVE SUMMARY

(ISC)² welcomes the Inquiry into Cybersecurity by the Legislative Council of the Parliament of New South Wales.

(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, the Certified Cloud Security Professional (CCSP®) certification, the Systems Security Certified Practitioner (SSCP®) certification, the Certified Secure Software Lifecycle Professional (CSSLP®) certification and the Healthcare Information Security and Privacy Practitioner (HCISPP®) certification, amongst others, (ISC)² offers a portfolio of credentials that are part of a holistic, programmatic approach to security. Our membership, more than 150,000 strong, with over 1,200 members in New South Wales and over 2,900 members in Australia, consists of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the cybersecurity, information security and privacy 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 the AS/NZS ISO/IEC 17024 Standard, a global benchmark for personnel certification. All (ISC)² certifications have been accredited against this standard, making (ISC)² credentials a must-have among information security professionals and employers. (ISC)² credentials are recognised by the United States Department of Defence (DoD) through the 8140.01 and 8570.1 Directives, the National Recognition Information Centre (NARIC) in the United Kingdom and European Union, the Australian Signals Directorate through the Information Security Registered Assessors Program (IRAP) and the Enhanced Competency Framework on Cybersecurity (ECF-C) by the Hong Kong Monetary Authority, to name a few.

In Australia, (ISC)² has formed strong, strategic partnerships with the Federal Government's Department of Home Affairs' Australian Cyber Security Centre (ACSC), the Australian Information Security Association (AISA) and the Australian Computer Society (ACS). In addition to this, partnerships have been formed with the New South Wales Government and the Victorian Government 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, TAFE NSW and TAFE Victoria as well as allied industry bodies including the Australian Security Industry Association (ASIAL), the IoT Alliance of Australia, the IoT Security Institute, the Australian Institute of Project Managers (AIPM), 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), the American National Standards Institute (ANSI) and National Institute for Cybersecurity Education (NICE) in the United States and the International Standards Organisation (ISO) at a global level. (ISC)² works closely with numerous government agencies and bodies across the Asia-Pacific region and around the world. Regional examples include the Cyber Security Agency of Singapore and the Tokyo Metropolitan Police Department in Japan. 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.

This response offered by (ISC)² represents the collective views of over 150,000 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 enterprises, NGO's as well as SME/SMBs across all industries, verticals and sectors.

It is our hope that the Legislative Council will consider the responses to the Terms of Reference and incorporate recommendations included as part of a holistic drive by the Parliament to help deliver a safer and more secure cyber world for the people of New South Wales, both now and well into the future.

TABLE OF CONTENTS

SUBMISSION INTRODUCTION

Core Information	Submitter Details
Name of Organisation	International Information Systems Security Certification Consortium, abbreviated to (ISC)^2
Contact for Further Enquiries	Tony Vizza Director of Cyber Security Advocacy, Asia-Pacific, (ISC)^2
Description of Organisation	(ISC)^2 is an international association of certified cyber security professionals offering certifications that are AS/NZS ISO/IEC 17024 accredited. Australian organisations rely on (ISC)^2 certified professionals to protect their information assets.
Specific areas of cyber security expertise	(ISC)^2 organises and collates the Common Body of Knowledge (CBK) for each cyber security certification administered by (ISC)^2. The CBK represents of the sum of all knowledge required to be proficient in a specific aspect of cyber security and is maintained and updated by the corps of working cyber security professionals within the domains that comprise each CBK.
Which sectors are main stakeholders?	All sectors that require information security personnel as an operational business need are considered stakeholders. The largest end customer for (ISC)^2 is the Government sector globally.

THE CYBER SECURITY LANDSCAPE FOR NSW TODAY

The current cyber threat environment is well documented both in Australia and globally. The gravity and severity of the cyber threat situation as it currently stands is best illustrated by World Economic Forum research that indicates that cyber security and privacy-related risks are listed as two of the top ten global risks in terms of likelihood and impact.[1] Conflating an already dire situation has been the Covid-19 pandemic that has resulted in a number of high-profile breaches and incidents have occurred within Australian organisations including breaches at Toll Group[2], BlueScope[3], Bigfooty.com[4], the NSW Government[5] and Lion Group[6] just to name a few.

The latest statistics published by the Australian Governments Office of the Australian Information Commissioner (OAIC) covering the period of January to June 2020 indicated a slight decrease of 3% in data breach notifications from the previous period (July to December 2019).[7] It should be noted, however, that the July to December 2019 period indicated the highest number of recorded notifications ever recorded by the OAIC.

These results are further reinforced by a report titled *ACSC Annual Cyber Threat Report* issued by the Australian Signals Directorate in conjunction with the Australian Federal Police and the Australian Criminal Intelligence Commission indicating that over 59,000 cybercrime reports were received in the 2019-20 financial year, with 2,266 incidents responded to by the Australian Cyber Security Centre.[8] In fact, the report illustrated that over the period, over 1,070 cyber incidents to organisations defined by DHA as critical were reported.[9]

The *ACSC Annual Cyber Threat Report* also illustrated that of the over 59,000 cybercrime reports received by law enforcement across Australia, 12,689 of those reports came from New South Wales.[10] The report also indicated that out of the 2,266 reports that were responded to by the Australian Cyber Security Centre, 367 of them came from state and territory governments. The report, however, does not distinguish between which state and territory governments those incidents came from.

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, the cyber threat environment will only erode further. Given this context, it is almost certain that cybersecurity will become a "Top 3" risk for organisations, rivalled only by climate change and global pandemics in terms of magnitude and impact out to 2030.

It is imperative that the NSW Government increase resilience and preparedness to cyber security issues. The role of government to act as an exemplar of good cyber security practice should not be understated and the economic and social benefit of achieving cyber resiliency in NSW should not be understated. The NSW government, representing the economic powerhouse of the nation has a particular role to play in inspiring and guiding other states and territories as well as the Federal Government in regulating for change, setting the pace and agenda by which the private sector and the public follow suit.

World Economic Forum *'Global Risk Report 2020* http //www3 we orum org/docs/WEF Global Risk Report 2020 pd

[2] News *'Toll Group s corporate data stolen by attackers* 12th May 2020 https //www itnews com au/news/toll-groups-corporate-data-stolen-by-attackers-548033

[3] ZDNet *'BlueScope reports cyber incident affecting Australian Operations* 18th May 2020 https //www zdnet com/article/bluescope-reports-cyber-incident-a ecting-australian-operations/

[4] Nine News *'Exclusive: 70 million records exposed in data leak from AFL fan website, cyber researchers claim* 29th May 2020 https //www 9news com au/national/a l- an-website-70m-data-leaks-expose-users-private-conversations-phone-numbers-emails/4b6 5c5c-7a76-4198-8e24-b90270 a 2b3

[5] ZDNet *'Citizen data compromised as Service NSW falls victim to phishing attack* 14th May 2020 https //www zdnet com/article/citizen-data-compromised-as-service-nsw- alls-victim-to-phishing-attack/

[6] Wire, *'Australian drinks maker Lion shuts systems after cyber incident* 10th June 2020 https //www itwire com/security/australian-drinks-maker-lion-shuts-systems-a ter-cyber-incident html

[7] O ice o the Australian n ormation Commissioner Australian Government *'Notifiable Data Breaches Report – January-June 2020* https //www oaic gov au/assets/privacy/noti iable-data-breaches-scheme/statistics/Noti iable-Data-Breaches-Report-Jan-Jun-2020 pd

[8] Australian Cyber Security Centre *'ACSC Annual Cyber Threat Report – July 2019 to June 2020* https //www cyber gov au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2019-june-2020

[9] bid Re er to page 7 his number includes all sectors listed as de ined by DHA as 'critical or the purposes o the consultation paper

[0] bid Re er to page 11

THE NSW GOVERNMENT CYBER SECURITY STRATEGY

THE 2018 STRATEGY AND A CHANGING WORLD

The current version of the NSW Cyber Security Strategy, dating back to 2018, provided a positive blueprint for Government to chart out and build cyber security policies, procedures and controls that sought to protect government services and aimed to protect the people of New South Wales.

While the 2018 NSW Cyber Security Strategy was detailed in its approach and aimed to provide a comprehensive strategy to manage cyber security risks using a whole-of-government lens, the world was very different just two short years ago. Since that time, Covid-19 has seen the world rapidly digitise to mitigate the huge levels of disruption seen in all sectors. The increased use of digital tools and resources has seen exponential growth in technologies such as cloud, BYOD (bring your own device) and mobile computing, just to name a few.

The rapid and massive shift to working from home has seen workers in both the public and private sectors connect to their workplaces remotely, often using their own computing devices and almost always using home networks where the general level of cyber security is often poor. This has now led to organisations and governments scrambling to implement cloud security, hardening of cyber defences for their datacentres, upscaling of remote network and telework capabilities and providing end user awareness campaigns around cybersecurity and privacy. Meanwhile, industry professionals across Australia have been calling on governments both state and federal to ensure that better cyber hygiene exists across all sectors of society.

A salient point to note regarding the link between the Covid-19 pandemic and cyber security is that an alarming spike in the number of cyber incidents being reported coincided with Covid-19 related lockdowns across Australia, with the *ACSC Annual Cyber Threat Report* indicating that April 2020 saw the largest number of recorded cyber security incidents across the 2019-20 reporting, with 318 incidents requiring Australian Cyber Security Centre assistance, almost double the previous months figure.[11] Research conducted by Cambridge University in the UK indicates that Covid-19 related lockdowns may have led to a sharp rise in workers concerned about their economic situation choosing to embrace cybercrime to make ends meet.[12]

In light of these developments, the NSW Government launched a call for views into the next iteration of the NSW Cyber Security Strategy in June 2020, coupled with an announcement of significant funding increases to the tune of $240 million over the next four years.[13] (ISC)[2] provided a detailed submission into this call for views with a comprehensive set of recommendations for the NSW Government to consider. This submission is contained in the Attachments section of this response.

Australian Cyber Security Centre *'ACSC Annual Cyber Threat Report – July 2019 to June 2020* Page 6 https //www cyber gov au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2019-june-2020

[2] University o Cambridge "Lockdown 'Helps uel rise in cybercrime " 3rd June 2020 https //www cam ac uk/research/news/lockdown-helps- uel-rise-in-cybercrime

[3] NSW Government '$180 million investment to expand NSW s cyber security 27th August 2020 https //www nsw gov au/news/180-million-investment-to-expand-nsws-cyber-security

FAILINGS IN THE CURRENT CYBER SECURITY APPROACH

Despite the existing 2018 NSW Cyber Security Strategy, a number of significant and serious data breaches have occurred either involving NSW Government departments or suppliers or affecting the reputation of the NSW Government including:

- Approximately 54,000 NSW drivers' licences and 108,535 other sensitive documents held by a private business unaffiliated to the NSW Government were hosted on a publicly available AWS cloud server in August 2020.[14]
- Over 3.8 million documents containing personal information relating to 186,000 NSW residents were breached due to a targeted phishing attack on 47 staff at Service NSW in April 2020. The total amount of data exfiltrated was over 738GB, a huge amount of data.[15]

These have occurred in light of the fact that according to the Commonwealth Government, the NSW Government has been singled out as a target by state sponsored attacks.[16]

In addition, in December of 2019, the Auditor-General for New South Wales has found significant shortfalls in the cyber preparedness of NSW Government departments.[17]

Another arguable area of weakness of the 2018 NSW Cyber Security Strategy was in its omission of a detailed strategy around cyber security education, awareness, accreditation and qualifications for NSW Government employees. An action item contained in the Strategy did consider the creation of standard cyber security job definitions,[18] however no such reference document seems to have been created since. Similarly, another action item, one that sought to create a cyber skills pathway model for NSW government agencies has not been produced, at least publicly, at the time of writing. Both of these actions would help bolster cyber security knowledge, skills and expertise within NSW Government if they were to be executed successfully. The reality of the cyber security ecosystem is that the human element of cyber security is the most effective element to address to improve outcomes, particularly given that the threat landscape is so complex and so vast, cyber security professionals need to have access to the right levels of training, accreditation and experience in order to perform their tasks diligently.

[4] Australian Broadcasting Corporation 'Data breach exposes tens o thousands o NSW driver s licences online 1st September 2020 https //www abc net au/news/2020-09-01/nsw-drivers-licence-data-breach-under-investigation/12611918

[5] News 'Service NSW reveals hackers stole 738GB o data in email compromise 7th September 2020 https //www itnews com au/news/service-nsw-reveals-hackers-stole-738gb-o -data-in-email-compromise-552932

[6] Sydney Morning Herald 'NSW Government was warned over cyber security weaknesses 20th June 2020 https //www smh com au/national/nsw/nsw-government-was-warned-over-cyber-security-weaknesses-20200620-p554iu html

[7] Audit O ice o New South Wales 'Central Agencies 2019 12th December 2019 https //www audit nsw gov au/our-work/reports/central-agencies-2019-0

[8] NSW Government 'Cyber Security Strategy A Cyber Sa e NSW 2018 Page 14
https //www digital nsw gov au/sites/de ault/ iles/NSW%20Cyber%20Security%20Strategy%202018 pd

RECOMMENDATIONS FOR CYBER SECURITY IMPROVEMENT

The fooling set of recommendations is derived from the (ISC)[2] submissions to both the NSW 2020 Cyber Security Strategy as well the Commonwealth Government's 2020 Cyber Security Strategy.

1 – ENDORSEMENT, PROMOTION AND ADOPTION OF ISO/IEC 27000:2018 FAMILY OF CYBER SECURITY CONTROLS

To achieve better cybersecurity resilience for organisations, **the NSW Government should endorse, promote and adopt the internationally accepted ISO/IEC 27000:2018 family of Information Security Management System accreditations,[19] both internally as well as for stakeholders such as suppliers as well as the broader NSW economy.**

The family of ISO/IEC 27000:2018 accreditations which should be endorsed, adopted and promoted includes ISO/IEC 27001 (Information technology — Security techniques — Information security management systems — Requirements), ISO/IEC 27005 (Information security risk management), ISO/IEC 27014 (Security Governance), ISO/IEC 27017 (Cloud Security) and ISO/IEC 27034 (Application security).

By adopting the ISO/IEC 27000 family of standards, the NSW government can demonstrate that its departments are capable of protecting the information security assets of their own operations as well as of their stakeholders. By adopting this recommendation, many of the actions listed in the Action Plan contained in the existing *NSW Government Cyber Security Strategy* will be met. Crucially, the NSW Government will lead by example.

2 – ENDORSEMENT, PROMOTION AND ADOPTION OF AS/NZS ISO/IEC 17024:2012 CYBER SECURITY PERSONNEL ACCREDITATIONS

To ensure that the cyber workforce and skills ecosystem across NSW is trained in globally recognised, quality-assured and industry relevant knowledge, **the NSW Government should endorse, promote and adopt the internationally accepted AS/NZS ISO/IEC 17024:2012 Personnel Accreditation[20] scheme**. This will ensure that cyber security professionals employed by the state of NSW are accredited in globally recognised cybersecurity certifications, such as those administered by (ISC)[2], all of which are AS/NZS ISO/IEC 17024 accredited. This will help meet a key theme as described in the *2018 NSW Cyber Security Industry Development Strategy*, that being of closing the cyber security workforce skills gap.

In addition, **the NSW Government should consider following the lead set by the Government of Victoria in mandating that all public sector staff who manage cyber security for Victorian Government departments are trained and certified in an AS/NZS ISO/IEC 17024 accredited certification.[21]** Since October 2019, the Victorian Government has actively been promoting the CISSP, SSCP and CCSP certifications administered by (ISC)[2], amongst others, to staff in their IT, cybersecurity and cloud security functions. This complements the Victorian Government strategy that all public sector workers, regardless of job role, be provided some level of cyber security awareness and training.

3 – INVESTMENT IN EDUCATION PROVIDERS TEACHING INDUSTRY RELEVANT CYBERSECURITY PROGRAMS

To increase the relevance and demand for cyber workforce and skills education programs offered by education institutions domiciled or operating in NSW, **the NSW Government should seek to capitalise on the global demand for cyber security skills, knowledge and experience by utilising the vast network of universities, TAFE and private sector providers in NSW to help address the cyber security skills shortage**, currently estimated by (ISC)[2] to be over 4 million people around the world, noting that most of this shortage exists in the Asia-Pacific region.[22]

In order to achieve this goal, **the NSW Government should mandate and/or incentivise universities, TAFE and private sector education providers to ensure that their cyber security educational programs align to global industry standards**

---

[9] nternational Standards Organisation (SO) ' SO/ EC 27000 2018 n ormation echnology – Security echniques – n ormation Security Management Systems – Overview and vocabulary https //www iso org/standard/73906 html

[20] nternational Standards Organisation (SO) ' SO/ EC 17024 2012 Con ormity Assessment – General Requirements or bodies operating certi ication o persons https //www iso org/standard/52993 html

[2] For urther in ormation please contact the Department o Premier and Cabinet Victorian Government – https //www vic gov au/department -premier-and-cabinet

[22] (SC)[2] 'Cybersecurity Work orce Study 2019 https //www isc2 org/Research/Work orce-Study

and needs, including the incorporation of AS/NZS ISO/IEC 17024 accredited certifications as part of their cyber programs. This will ensure that graduates possess globally recognised, industry accredited, in demand and quality cyber security skills that are easily transferable between employers and are universally recognised by private and public sector institutions both across Australia and around the world.

In adopting this recommendation, the NSW Government will help ensure that graduates from NSW universities, TAFE NSW or accredited private sector providers possess relevant skills, established experience and prudent mindset required to be effective cyber security professionals. This will establish NSW as a regional centre of cyber security excellence and will further ensure that the state of NSW becomes a net exporter of high-quality cyber security workers to the Asia-Pacific region and the wider world.

4 – ADOPTION OF RECOGNISED CYBERSECURITY SKILLS FRAMEWORKS

Cybersecurity is a vast area comprising of a number of different skills needed to ensure that organisations adequately protect from, detect and respond to cyber incidents. In recognising this, **the NSW Government should consider the adoption of the Commonwealth Government's Australian Signals Directorate's *Cyber Skills Framework***[23] released in September 2020, which leverages the widely adopted and highly regarded US Government National Institute for Cybersecurity Education (NICE) Framework.[24] By adopting the *Cyber Skills Framework,* the NSW Government will leverage a standardised reference structure that describes the interdisciplinary nature of the knowledge, skills and abilities required to perform all aspects of cyber security work, including technical, operational, management, governance, risk and compliance based cybersecurity work. This will also ensure that the NSW Government is cognisant of which knowledge, skills and abilities are valuable and consistent with best practice as deemed by the Australian Signals Directorate as well as through NICE.

5 – SUPPORTING, PROMOTING AND USING LOCALLY MADE AND OWNED CYBERSECURITY AND INFORMATION TECHNOLOGY PRODUCTS AND SERVICES

As nation states seek to develop (or in many cases re-develop) sovereign manufacturing capabilities in the aftermath of the COVID-19 pandemic and its economic and national security after-effects, a strong local cyber security and information technology sector is vital for the long-term success of the NSW economy as well as the broader Australian economy, which is heavily reliant on NSW as a driver of economic growth.

In order to achieve the aim of business growth and innovation, **the NSW Government should consider supporting, promoting and using locally made, owned or recognised cyber security and world-leading information technology products and services.** Recommendations to help achieve this goal include:

- The NSW Government subsidising the costs of ISO/IEC 27000:2018[25] certification for locally based and owned businesses that provide cybersecurity and IT products and services to ensure that those organisations are employing best practice information security management techniques.
- The NSW Government subsidising the costs of AS/NZS ISO/IEC 17024:2012[26] personnel certification for locally based and owned businesses that provide cybersecurity and IT products and services to ensure that the personnel working in these organisations are globally recognised experts in their field.
- NSW Government procurement preferring to use locally based, owned and ISO/IEC 27000:2018 certified businesses that provide cybersecurity and IT products and services wherever possible for public-sector needs in order to assist the local cyber and IT ecosystem grow and thrive.
- The NSW Government actively working with AustCyber to help promote innovative and locally made cybersecurity products and services to the Asia-Pacific region and the global market.

---

[23] Australian Signals Directorate 'ASD Cyber Skills Framework https //www cyber gov au/acsc/view-all-content/publications/asd-cyber-skills- ramework
[24] National nitiative or Cybersecurity Education (N CE) U S Department o Commerce United States Government 'N S Special Publication 800-181 National nitiative or Cybersecurity Education (N CE) Cybersecurity Work orce Framework https //nvlpubs nist gov/nistpubs/SpecialPublications/N S SP 800-181 pd
[25] nternational Standards Organisation (SO) ' SO/ EC 27000 2018 n ormation echnology – Security echniques – n ormation Security Management Systems – Overview and vocabulary https //www iso org/standard/73906 html
[26] nternational Standards Organisation (SO) ' SO/ EC 17024 2012 Con ormity Assessment – General Requirements or bodies operating certi ication o persons https //www iso org/standard/52993 html

6 – SETTING APPROPRIATE LEVELS OF INFORMATION SECURITY EXPECTATIONS IN THE PRIVATE SECTOR

In order to achieve the aims of resilience, workforce and skills, business growth and innovation, **the NSW Government should consider setting the appropriate levels of expectation in relation to how external stakeholders in the private sector conduct themselves regarding their information security posture,** particularly when engaging with the NSW Government and its departments. Recommendations to help achieve this goal include:

- The NSW Government subsidising the cost of ISO/IEC 27000:2018 certification for locally based and owned private sector and not-for-profit entities to ensure that those organisations are employing best practice information security management practices and techniques in their day-to-day business.
- The NSW Government subsidising the costs of AS/NZS ISO/IEC 17024:2012 personnel certification for locally based and owned private sector and not-for-profit entities to ensure that personnel working in these organisations protecting information assets are experienced, ethical and verified experts in their field.
- NSW Government procurement preferring to use ISO/IEC 27000:2018 certified suppliers for all procurement wherever possible to promote the adoption of appropriate information security management controls amongst the broader NSW business ecosystem.
- NSW Government restricting access to sensitive NSW government services to external stakeholders and third parties until such time as those third parties can adequately attest to the resiliency of their own information security controls. Examples of this include:
    - Restricting access to systems such as the NSW Land Registry Services, the Rental Bond Board and Health Services, for example, only to organisations that have demonstrated a minimum baseline of cyber security hygiene.
    - Creating a cyber security version of a scheme similar to the NSW Food Authority's 'Name and Shame' register used for businesses that have breached food safety laws[27] in instances where organisations have suffered repeated data breaches.

7 – MODERNISING AND STRENGTHENING PRIVACY PROVISIONS AND REGULATIONS

Many jurisdictions around the world have strengthened privacy rules to ensure that citizens are able to use technology and exercising a level of privacy that they deem acceptable. **The NSW Government should consider modernising the State Governments *Privacy and Personal Information Protection Act* 1994 (NSW), *Health Records and Information Privacy Act 2002* (NSW) and promote reform of the Commonwealth *Privacy Act 1988* through the National Cabinet** to ensure that the privacy needs of individuals and businesses are met in today's digital era.

As guidance, the NSW Government should refer to the European Union's General Data Protection Regulation (GDPR)[28] and the *California Consumer Privacy Act of 2018*[29] as good examples for such reform.[30]

8 – IMPLEMENTING REGULATIONS REQUIRING MINIMUM LEVELS OF CYBER SECURITY FOR CONSUMERS

The NSW government should consider the adoption of regulations that ensure that NSW based manufacturers of information technology products incorporate best practice cyber security protections within the products they manufacture and/or distribute to ensure those products meet a minimum level of protection for consumers. The state legislature of California in the United States has legislated Senate Bill No. 327[31], popularly known as the '*IoT Security Law*' offering consumers appropriate levels of protection, and the NSW Government should adopt regulations at a state level or pursue the matter through the National Cabinet to promote the adoption of similar regulation at a federal level to ensure IT products are fit for sale to NSW consumers.

---

[27] NSW Food Authority - NSW Government 'Name and Shame https //www oodauthority nsw gov au/o ences

[28] European Commission 'EU data protection rules https //ec europa eu/commission/priorities/justice-and- undamental-rights/data-protection/2018-re orm-eu-data-protection-rules en

[29] *California Consumer Privacy Act of 2018,* 160 Cal Civ Code § 1798 100 – 1798 199 (2018)

[30] European Commission 'EU data protection rules https //ec europa eu/commission/priorities/justice-and- undamental-rights/data-protection/2018-re orm-eu-data-protection-rules en

[3] *Senate Bill No. 327 Information Privacy: Connected Devices* (Cali ornia) https //legin o legislature ca gov/ aces/bill extClient xhtml?bill id=201720180SB327

9 – PARTNERING WITH GLOBALLY RECOGNISED INTERNATIONAL INDUSTRY BODIES AND ASSOCIATIONS

The NSW Government should partner with globally recognised international industry bodies and associations such as (ISC)² and encourage academic institutions and the private sector do the same. This will ensure that strong alignment exists between the NSW Government and the broader global cyber security community represented by cybersecurity professionals and professional bodies that represent the cybersecurity industry.

By partnering with global peak industry bodies, the relevance of measures that the NSW Government is undertaking can be showcased at an international level. It offers the NSW Government a route to showcase innovative home-grown products and services to a wider audience and will ensure that will further ensure that the cyber skills gap in NSW is systematically addressed and converted into a regionally and globally strategic advantage.

10 – ADOPTION AND PROMOTION OF STANDARDISED CYBERSECURITY INDUSTRY LEXICON

To improve inter-government and government-industry relationships, **the NSW Government should consider promoting the standardisation across government and industry of cyber security concepts and technologies through a common industry lexicon**. An example of such a lexicon is the *(ISC)² Cybersecurity Lexicon*.[32]

[32] he (SC)² Cybersecurity Lexicon – An introduction to basic cybersecurity terminology and concepts https //www isc2 org/-/media/ SC2/ raining/ he- SC2-Cybersecurity-Lexicon ashx

ABOUT THE LEAD AUTHOR

Tony Vizza
Director for Cyber Security Advocacy
Asia-Pacific
(ISC)²

Tony Vizza has been involved in the information technology, information security and privacy fields for more than 25 years.

Tony has completed a Bachelor of Science in Computing Science from the University of Technology, Sydney and a Global Executive MBA from the University of Sydney which included study at Stanford University in the United States, The London School of Economics in the UK and the Indian Institute of Management, Bangalore in India. Tony is currently studying for a Juris Doctor law degree at the University of New South Wales.

Tony's information security credentials include CISSP (Certified Information Systems Security Professional), CCSP (Certified Cloud Security Professional), CIPP/E (Certified Information Privacy Professional / Europe), CRISC (Certified in Risk and Information Systems Controls), CISM (Certified Information Security Manager) and he is a certified ISO/IEC 27001 Senior Lead Auditor.

Tony is a member of the Board of Directors for the Australian Information Security Association (AISA), a Cyber Security Ambassador for the NSW Government, the co-chair for the (ISC)² Asia-Pacific Advisory Council, a member of the Cybersecurity Industry Advisory Council for the NSW Government, a member of the Technology and Business Services Industry Skills Reference Group for NSW TAFE, a member of the Data Security Standards Committee for Blockchain Australia and has provided expert services to the Australian Government's Australian Prudential Regulation Authority (APRA), the Law Society of NSW, the Australian Security Industry Association Limited (ASIAL), the Australian Institute of Project Management (AIPM) as well as numerous boards.

Tony is an expert speaker on information security regularly speaking across the Asia-Pacific region on information security matters. He has also taught and mentored young and aspiring information security students through Victoria University, TAFE NSW and TAFE Victoria in association with Infoxchange and has lectured cybersecurity students at the University of Technology, Sydney, the University of New South Wales and the University of Queensland.

Tony is a regular contributor to numerous cyber security and IT industry publications including CSO Magazine, Infosecurity Magazine, Cyber Today Australia, Security Insider Magazine, Australian Reseller News (ARN), Channel Reseller News (CRN) and Lifehacker, amongst others, regarding information security, business and channel strategy.

ATTACHMENTS

1) (ISC)^2 SUBMISSION TO THE 2020 NSW GOVERNMENT CYBER SECURITY STRATEGY