



**STRENGTHENING
AUSTRALIA'S
CYBER SECURITY
REGULATIONS
& INCENTIVES
SUBMISSION**



AUSTRALIAN INFORMATION SECURITY ASSOCIATION

About AISA

The Australian Information Security Association (AISA) welcomes the request for the call for views from the Australian Government's Department of Home Affairs in relation to strengthening Australia's cyber security regulations and incentives. The Australian Government opened consultation on options for regulatory reforms and voluntary incentives to strengthen the cyber security of Australia's digital economy. AISA understands the government is focusing on three core areas: setting clear cyber security expectations through standards for corporate governance, personal information, and smart devices; increasing transparency of cyber security maturity / capability in the market and finally; protecting consumer rights through appropriate legal remedies for victims.

AISA champions the development of a robust information security sector by building the capacity of professionals in Australia and advancing the cyber security and safety of the Australian public as well as businesses and governments in Australia. Established in 1999 as a nationally recognised and independent not-for-profit organisation and charity, AISA has become the recognised authority and industry body for information security, cyber security, and privacy in Australia. AISA caters to all domains of the information security industry with a particular focus on sharing expertise from the field at meetings, focus groups and networking opportunities around Australia.

AISA's vision is a world where all people, businesses and governments are educated about the risks and dangers of cyber-attack and data theft, and to enable them to take all reasonable precautions to protect themselves. AISA was created to provide leadership for the development, promotion, and improvement of our profession, and AISA's strategic plan calls for continued work in the areas of advocacy, diversity, education, and organisational excellence.

This response offered by AISA represents the collective views of over 7,500 cyber security and information technology professionals, board directors, allied professionals in industries such as the legal, regulatory, financial and prudential sector, as well as cyber and IT enthusiasts Australia. AISA members are tasked with protecting and securing public and private sector organisations including national, state and local governments, ASX listed companies, large enterprises, NGO's as well as SME/SMBs across all industries, verticals and sectors.

AISA proactively works to achieve its mission along with its strategic partners. These include the Australian Cyber Security Centre, AustCyber, Cyrise, the Risk Management Institute of Australia (RMIA), the Australian Strategic Policy Institute (ASPI), the Australian Institute of Company Directors (AICD), the Oceania Cyber Security Centre (OCSC), the Australian Security Industry Association Limited (ASIAL) as well as international partner associations such as (ISC)², the Centre for Cyber Safety and Education, ISACA, IAPP, the Association of Information Security Professionals (AiSP), the IoT Security Institute (IoTSI) and over twenty five Universities and TAFEs across Australia.

It is AISA's hope that the Department of Home Affairs will consider our responses to the call for views and incorporate recommendations included as part of a holistic drive by the Australian Government to help deliver a safer and more secure cyber world for the people of Australia, both now and well into the future.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	5
RAISING OUR CYBER SECURITY POSTURE, REGULATING FOR PURPOSE	5
HIGH LEVEL FINDINGS.....	6
PRINCIPLES FOR CYBER SECURITY REFORM	8
WHY SHOULD GOVERNMENT TAKE ACTION?	9
1. WHAT ARE THE FACTORS PREVENTING THE ADOPTION OF CYBER SECURITY BEST PRACTICE IN AUSTRALIA?	9
2. DO NEGATIVE EXTERNALITIES AND INFORMATION ASYMMETRIES CREATE A NEED FOR GOVERNMENT ACTION ON CYBER SECURITY? WHY OR WHY NOT?.....	12
.....	13
THE CURRENT REGULATORY FRAMEWORK	14
3. WHAT ARE THE STRENGTHS AND LIMITATIONS OF AUSTRALIA’S CURRENT REGULATORY FRAMEWORK FOR CYBER SECURITY?	14
4. HOW COULD AUSTRALIA’S CURRENT REGULATORY ENVIRONMENT EVOLVE TO IMPROVE CLARITY, COVERAGE AND ENFORCEMENT OF CYBER SECURITY REQUIREMENTS?	16
GOVERNANCE STANDARDS FOR LARGE BUSINESSES	16
5. WHAT IS THE BEST APPROACH TO STRENGTHENING CORPORATE GOVERNANCE OF CYBER SECURITY RISK? WHY?	16
6. WHAT CYBER SECURITY SUPPORT, IF ANY, SHOULD BE PROVIDED TO DIRECTORS OF SMALL AND MEDIUM COMPANIES?	17
7. ARE ADDITIONAL EDUCATION AND AWARENESS RAISING INITIATIVES FOR SENIOR BUSINESS LEADERS REQUIRED? WHAT SHOULD THIS LOOK LIKE?	18
MINIMUM STANDARDS FOR PERSONAL INFORMATION	19
8. WOULD A CYBER SECURITY CODE UNDER THE PRIVACY ACT BE AN EFFECTIVE WAY TO PROMOTE THE UPTAKE OF CYBER SECURITY STANDARDS IN AUSTRALIA? IF NOT, WHAT OTHER APPROACH COULD BE TAKEN?.....	19
9. WHAT COST EFFECTIVE AND ACHIEVABLE TECHNICAL CONTROLS COULD BE INCLUDED AS PART OF A CODE UNDER THE PRIVACY ACT (INCLUDING ANY SPECIFIC STANDARDS)?.....	19
10. WHAT TECHNOLOGIES, SECTORS OR TYPES OF DATA SHOULD BE COVERED BY A CODE UNDER THE PRIVACY ACT TO ACHIEVE THE BEST CYBER SECURITY OUTCOMES?	20
STANDARDS FOR SMART DEVICES	21
11. WHAT IS THE BEST APPROACH TO STRENGTHENING THE CYBER SECURITY OF SMART DEVICES?	21
12. WOULD ESTI EN 303 645 BE AN APPROPRIATE INTERNATIONAL STANDARD FOR AUSTRALIA TO ADOPT FOR AS A STANDARD FOR SMART DEVICES?.....	21
13. WOULD YOU BE WILLING TO VOLUNTARILY REMOVE SMART PRODUCTS FROM YOUR MARKETPLACE THAT DO NOT COMPLY WITH A SECURITY STANDARD?.....	22
15. IS A STANDARD FOR SMART DEVICES LIKELY TO HAVE UNINTENDED CONSEQUENCES ON THE AUSTRALIAN MARKET?	24
LABELLING FOR SMART DEVICES.....	25
16. WHAT IS THE BEST APPROACH TO ENCOURAGING CONSUMERS TO PURCHASE SECURE SMART DEVICES?.....	25
17. WOULD A COMBINATION OF LABELLING AND STANDARDS FOR SMART DEVICES BE A PRACTICAL AND EFFECTIVE APPROACH? WHY OR WHY NOT?	28
18. IS THERE LIKELY TO BE SUFFICIENT INDUSTRY UPTAKE OF A VOLUNTARY LABEL FOR SMART DEVICES? WHY OR WHY NOT? A. IF SO, WHICH EXISTING LABELLING SCHEME SHOULD AUSTRALIA SEEK TO FOLLOW?	28
19. WOULD A SECURITY EXPIRY DATE LABEL BE MOST APPROPRIATE FOR A MANDATORY LABELLING SCHEME FOR SMART DEVICES? WHY OR WHY NOT?	29

20. SHOULD A MANDATORY LABELLING SCHEME COVER MOBILE PHONES, AS WELL AS OTHER SMART DEVICES? WHY OR WHY NOT?	30
21. WOULD IT BE BENEFICIAL FOR MANUFACTURERS TO LABEL SMART DEVICES BOTH DIGITALLY AND PHYSICALLY? WHY OR WHY NOT?	30

RESPONSIBLE DISCLOSURE POLICIES31

22. WOULD VOLUNTARY GUIDANCE ENCOURAGE AUSTRALIAN BUSINESSES TO IMPLEMENT RESPONSIBLE DISCLOSURE POLICIES? IF NOT, WHAT ALTERNATIVE APPROACHES SHOULD BE CONSIDERED?	31
--	----

HEALTH CHECKS FOR SMALL BUSINESSES31

23. WOULD A CYBER SECURITY HEALTH CHECK PROGRAM IMPROVE AUSTRALIA’S CYBER SECURITY? IF NOT, WHAT OTHER APPROACH COULD BE TAKEN TO IMPROVE SUPPLY CHAIN MANAGEMENT FOR SMALL BUSINESSES?	31
24. WOULD SMALL BUSINESSES BENEFIT COMMERCIALY FROM A HEALTH CHECK PROGRAM? HOW ELSE COULD WE ENCOURAGE SMALL BUSINESSES TO PARTICIPATE IN A HEALTH CHECK PROGRAM?	32
CURRENT SME PROFILE ON A PAGE - PROVIDED BY DEBRA BORDIGNON, DIRECTOR OF DEAKIN’S DIGITAL INNOVATION FOR SME HUB (DISH).	33
25. IF THERE ANYTHING ELSE WE SHOULD CONSIDER IN THE DESIGN OF A HEALTH CHECK PROGRAM?	34

CLEAR LEGAL REMEDIES FOR CONSUMERS35

26. WHAT ISSUES HAVE ARISEN TO DEMONSTRATE ANY GAPS IN THE AUSTRALIAN CONSUMER LAW IN TERMS OF ITS APPLICATION TO DIGITAL PRODUCTS AND CYBER SECURITY RISK?	35
27. ARE THE REFORMS ALREADY BEING CONSIDERED TO PROTECT CONSUMERS ONLINE THROUGH THE PRIVACY ACT 1988 AND THE AUSTRALIAN CONSUMER LAW SUFFICIENT FOR CYBER SECURITY? WHAT OTHER ACTION SHOULD THE GOVERNMENT CONSIDER, IF ANY?	35

OTHER ISSUES36

28. WHAT OTHER POLICIES SHOULD WE CONSIDER TO SET CLEAR MINIMUM CYBER SECURITY EXPECTATIONS, INCREASE TRANSPARENCY AND DISCLOSURE, AND PROTECT THE RIGHTS CONSUMERS?	36
RANSOMWARE	36

AUTHORS37

ABOUT THE LEAD AUTHORS	37
------------------------------	----

Executive Summary

Raising our Cyber Security Posture, Regulating for Purpose

Cyber security continues to be a concern internationally, with major cyber incidents and state-sponsored attacks attracting policy and industry focus across likeminded nations. The private sector is particularly impacted when cyber risks materialise. Directors and Officers of companies are in a unique position. They have a vested interest in ensuring the safety and security of their customers, workforce, and intellectual property (IP); obligations they increasingly take seriously.

The Australian Government, through parallel statutory and policy reform processes, is seeking to respond to the contextual issues it has identified as important in relation to cyber security.

To inform this process, in mid-2021, the Australian Information Security Association (AISA) undertook surveys of Directors of listed and non-listed Australian companies, as well as public institutions, NGOs, cyber professionals and executives across an audience of over 7,000 individuals. Further AustCyber has received qualitative feedback on the key issues at hand.

Jointly, AustCyber and AISA analysed these collective responses, including qualitative feedback received, to provide an overview of the perceived cyber risks and complexities in the practice of cyber security facing directors, boards, and companies. From this feedback, we identified salient themes in relation to how respondents felt Government, and indeed industry, should respond and better engage across stakeholders. These can be read alongside the Recommendations Report of the NSW Cyber Security Standards Harmonisation Taskforce, released in early 2021 which outlines a range of existing standards in existence, including in specific sectors of the economy.

To provide a framing for Government as these policy, regulatory and legislative reforms are considered, we outline a set of common principles to assist decision-makers. These are not intended to be exhaustive, but to function as a baseline. We look forward to further engagement with our respective Members and Stakeholders, to evolve these principles as the reforms being proposed by Government are considered.

High level findings

Directors, Executives and Key Staff are concerned about cyber security risks:

- 54% of survey respondents indicated they are 'extremely concerned' about the risk of cyber security breaches within their organisation.

Customers, not Governments alone, create a driver to improve cyber security posture:

- 51% of survey respondents reported that 'to a large extent' they 'felt pressure to act' on cyber security risks due to customer sentiment (cf. 31% for Government and regulators).
- Qualitative discussions identified increasing customer awareness for the need to expect more from suppliers on cyber security and privacy

There is emerging sentiment that boards are increasingly equipped to respond to cyber security risks:

- 76% of survey respondents 'strongly agreed' or 'somewhat agreed' that their board has adequate experience to address the cyber security risks facing their organisation.
- 60% of qualitative discussions noted the need for any messaging and/ or activities directed to boards to also be packaged in a way that is suitable for heads of organisations that do not have a board. This also holds true for helping organisations currently without a board which are likely to form a board in future stages of growth.

Entities are increasingly taking proactive measures to ensure cyber security:

- 70% of survey respondents, for example, had embedded 'cyber security into risk management frameworks'
- 57% has received board reporting on 'cyber security exposures/ risks.'

There is broad support for education and training, as well as industry and sector-specific guidance materials, specifically for directors, on cyber security risks:

- 78.4% of survey respondents supported better education and training for directors
- 64.7% supported general better practice guidance from industry
- 56.9% wanted sector specific better practice guidance

There are gaps, including those based on information asymmetries, for sections of the economy, that need to be addressed. Comments include:

"We provide consulting and managed security services to small and medium business. There remain vast inadequacies in available information and assistance to SME for implementation, development and maturity of Cyber Security policies, capability, and compliance. We'd like to see programs that address these issues in both large enterprise and small business context, using appropriate language, taking account that most small business does not have security staff or knowledge at management levels."

"Given the majority of Australian businesses cannot afford cyber security consultants, let alone understand the jargon, effort needs to be directed in making cyber security consultants accessible to SME businesses through some type of Government rebate for SME businesses who demonstrate a level of cyber security."

Respondents are concerned that some of the measures proposed might fracture the existing cyber security regulatory regimes that exist and create duplication in some instances. Comments include:

“Mature segments of the industry understand our threat landscape and the practicalities of security controls better than a government dept.. Additionally, need to ensure alignment with existing mandatory security obligations. e.g., will DHA's new PSOs under the SOCI amendment conflict with or align with APRA's CPS 234 for the fin. services industry?”

“Mandating cyber standards will drive the same risk avoidance culture as we see in OHS/WHS. This will in turn create additional cost burdens on businesses in an already tight market environment. Whilst we might wring our hands in horror, unlike in WHS/OHS... in 99% of cases people don't die from cyber incidents. Legislation and forced mandates must be reserved only for where there is a realistic direct risk that somebody might die as a result of the cyber-attack[...] A better approach is to make the market work better by improving transparency so that buyers and sellers are on an even playing field.”

“Regulatory standards at a Federal level must be considered in relation to State laws. The opportunity for regulatory duplication is already evident in SoCI. Is this to be a standard designed and supported by an Australian only remit, or will it encompass IEC, NIST or other standards?”

Respondents have provided constructive ideas as to how statutory regulatory and policy measures can leverage industry good practice. Comments provided include:

“From experience, a dual approach works best for organisations: 1. A set of minimal common sense general standards that can be quickly implemented, measured and enforced e.g. quality backups. 2. A risk-based framework for determining longer term additional measures, or fine tuning, based on data sensitivity analysis i.e., the owners of the data get to decide data sensitivity ratings based on potential business impacts related to data breaches and the IT security team get to decide the most cost-effective measures to match the sensitivity ratings. The higher the rating, the stronger collective controls need to be.”

“We shouldn't need to recreate (again) standards that already exist, such as ISO 27001 which is already risk based and does not prescribe what controls are implemented. If Legislation was clear, unambiguous, and referenced standards that it trusts to demonstrate 'adequate' security then that would help a great deal. I do not see the point of just pointing to 'Voluntary standards' as we have that already.”

“Any legislation brought forward must be in consultation with a wide sector of industry, not just cyber security practitioners. Any mandatory reporting requirement of breaches of any type must have assurances on the privacy and confidentiality of such reporting.”

Principles for cyber security reform

Based on the findings coupled with the detailed comments received from directors and business executives, AISA proposes the following principles be adopted by Government as it considers policy and regulatory reforms in relation to cyber security in Australia.

- 1. Policy responses should be proportionate to the magnitude of the specific risk(s) the proposal(s) seek to address, recognising the highly contextual nature of cyber security risk. Regulatory Impact Statements (RIS) should be developed and disclosed on key proposals to enable deep industry engagement and clear visibility of the intersections between regulatory and legislative measures.**

This will be especially beneficial for younger companies, as they mature how they engage with Government and how they interact with the public policy making process.

- 2. Policy, regulatory and other responses should avoid duplication, regardless of whether they are voluntary or mandatory (i.e., statutory measures). Wherever possible, responses should leverage existing industry good practice, including recognised international standards, some of which are already used at-scale.**

This will help support ongoing improvements to global competitiveness of all industries, including the cyber security industry itself, and ensure relevance by Australian organisations to the international cyber ecosystem

- 3. Co-design processes should be an embedded practice in regulatory and legislative development and adjustment. Industry consultation should be broad and cross-sectoral, to enable consideration, analysis, and input from all sectors of the economy. Technical experts alone cannot, nor should they, be expected to determine and shape enterprise level responses to cyber security risks, however, will be essential to consult in this process**

- 4. There should be adequate consideration of the needs of entities of different sizes and market orientation (domestic and/ or export), including those of micro and small businesses, and their varying levels of cyber maturity. The latter also applies to smaller government agencies and LGAs.**

This ensures policy and other measures are appropriate and any aspects of market failure are addressed in the most cost-effective way, both for businesses and the Government.

This is important for sectors the government views as critical or substantive who traditionally have not focused on cyber security capability or maturity (e.g. Education, Health, Food etc..) or had a need to build this capability. As an example the financial sector has had over 20 years to build capability and maturity while other sectors are just starting the journey.

- 5. Provide for adequate independent regulatory mechanisms and funding to ensure the legislation is effective.**

Today we already have underfunded regulators, so adding to their mission without commensurate increases in funding will result in suboptimal outcomes. Legislation should

only be introduced to Parliament if it is accompanied by actual appropriation of funds to regulators.

Why Should Government Take Action?

AISA has endeavoured to answer each of the questions based on AISA Member Survey data, consultation with industry partners, industry leaders, AISA's Executive Advisory Board, and though AISA's National Board Advocacy and Policy perspectives of the authors in conjunction with AustCyber.

1. What are the factors preventing the adoption of cyber security best practice in Australia?

AISA believes there are multiple contributing factors that hinder and prevent the adoption of best practice cyber security in Australia.

1 - Lack of standards-based cyber security guidance as well as conflicting advice provided to industry and the public as to how to best protect information assets.

The landscape of cyber security standards across the Australian cyber security ecosystem is often confusing, difficult to understand and contradictory. This sometimes results in poor implementation of cyber security policy, which eventuates in poor cyber security outcomes.

In relation to the Commonwealth Government, federal departments are required to conform to the Australian Signals Directorate (ASD) Information Security Manual (ISM).¹ While the ISM is based on internationally accepted cyber security standards such as ISO27001 and NIST 800-37, the ISM itself is an Australia-specific document with little to no relevance at a global level, reducing the effectiveness of it as a standard compared to its globally accepted peers. If State government guidance is taken into consideration, differing State standards exist from both the Commonwealth, as well as between each state or territory.

To illustrate the complex patchwork of policies and standards that exist today, New South Wales uses the NSW Cyber Security Policy² which mandates 25 controls; Queensland,³ South Australia,⁴ Western Australia⁵ and Tasmania⁶ use ISO27001 which allows for a statement of applicability dependent on the needs and specifics of each department. Meanwhile, Victoria uses the Victorian Protective Data Security Standards V2.0 (VPDSS)⁷ with 12 discrete controls. This clear lack of uniformity between jurisdictions creates unnecessary confusion for the private sector, non-government, as well as government entities – all which are seeking to manage cyber security issues that do not differ in any way between jurisdictions.

Adding to the array of standards that exist across the Australian ecosystem, industry-specific regimes exist that are not related to those promoted by state or commonwealth governments. For example, APRA regulated entities must conform to Prudential Standard CPS-234,⁸ which aims to

1 https://www.cyber.gov.au/acsc/view-all-content/ism_

2 <https://www.digital.nsw.gov.au/sites/default/files/NSW%20Cyber%20Security%20Policy%202021%204.0.pdf>.

3 <https://www.qgocio.qld.gov.au/documents/information-security-policy>.

4 https://www.dpc.sa.gov.au/__data/assets/pdf_file/0017/126116/South-Australian-Cyber-Security-Framework.pdf page 9.

5 <https://www.wa.gov.au/sites/default/files/2018-06/Digital%20security%20policy%20-%20supplementary%20guide.pdf> page 4.

6 http://www.dpac.tas.gov.au/__data/assets/pdf_file/0003/476706/Tasmanian_Government_Cybersecurity_Policy.pdf page 6.

7 <https://ovic.vic.gov.au/data-protection/standards/>.

8 https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf.

cater for the wide variety of organisations that are regulated by APRA, written from a business perspective does not reference any industry or internationally accepted standard.

To add further complexity, the ACSC recommends 'Essential Strategies to Mitigate Cyber Security Incidents' to help organisations protect themselves against various cyber threats including specifically the 'ASD Essential Eight' designed to predominantly protect Microsoft Windows-based internet-connected networks. While the ASD Essential Eight are drawn from the ISM, there is no reciprocity either in terms of the ASD Essential Eight or the Essential Eight Maturity Model with internationally respected standards such as ISO27001 or internationally emerging models such as the Cybersecurity Maturity Model Certification (CMMC).⁹ The ASD Essential Eight is also based purely on technical controls and gives little consideration to cultural or cyber awareness. Additionally, more diverse organisations use cloud services as well as the outsourcing of IT processes. By pushing IT controls only, the ASD Essential Eight continues to perpetuate the misconception in organisations that cyber security is simply an IT issue, rather than framing cyber security as a business risk to be managed holistically by directors, executives, suppliers and staff.

RECOMMENDATIONS

- Establish a formal baseline cyber security standard guidance for Australian Governments (both Federal, State and Territory) based on globally recognised industry standards.
- Mandate this standard at Federal and State Government level by legislation.
- Based on this chosen and adopted standard, provide guidance customised by industry sector.

2 - A lack of professionalisation of the Australian cyber security workforce.

AISA believes that the cyber security sector requires strong input and direction from Government in relation to the educational and experiential requirements by individuals that are employed in the sector.

There are currently no official positions, policies, or standards in relation to what level of qualification or accreditation is necessary to be deemed a 'cyber security professional' operating in Australia, nor is there any official guidance in relation to codes of ethics or conduct expected from individuals employed in the cyber security workforce.

While previous attempts at professionalisation of the workforce have occurred, broadly speaking, these have been unsuccessful. The Australian Computer Society (ACS), a body accredited by the statutorily recognised Professional Standards Council,¹⁰ has established a Certified Technologist / Certified Professional designation in the Cyber Security field.¹¹ However, uptake of these designations has been minimal with less than 80 certified cyber / information security professionals listed on the ACS register.¹² AISA notes that the cyber security sector has over 300¹³ globally recognised certifications and contends that another local Australian one (as designed by the ACS) is not necessary or required.

⁹ https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf.

¹⁰ <https://www.psc.gov.au/professional-standards-schemes/scheme-documents>.

¹¹ <https://www.acs.org.au/professionalrecognition/certification-landing-page.html>. Please refer to 'FAQS Cyber-Security'.

¹² <https://www.acs.org.au/solutionsforemployers/cp-directory.html> - using search term 'cyber' and 'security'.

¹³ <https://pauljerimy.com/security-certification-roadmap/>

In relation to certifications formally sanctioned by the Australian government, the Information Security Registered Assessors Program (IRAP) accreditation,¹⁴ operated by the ASD, is the only explicitly designated official certification program related to cyber security operating in Australia today. However, it represents a niche aspect of cyber security related only to auditing government information systems and due to the existing dimensions of the program, it tends to operate only in the area of essential advisory and auditing of entities that are required to have an IRAP assessor undertake the audit. As a result, there are only approximately 150 certified IRAP assessors in Australia today.

AISA contends that there is critical need for government to provide guidance to industry in relation to what knowledge, skills, and abilities a cyber security professional should possess. AISA notes that the ASD Cyber Skills Framework¹⁵ attempts to address the specific knowledge, skills, and abilities different roles in cyber security should possess and at what level of proficiency. However, uptake of the Framework has been minimal. In addition, there is significant confusion in relation to other skills frameworks that are promoted by various entities and agencies. For example, AustCyber, funded by the Commonwealth, heavily promotes the US-based National Initiative for Cybersecurity Education (NICE) Framework¹⁶ while the Federal Governments Digital Transformation Agency (DTA) are strongly aligned with the Skills for the Information Age (SFIA) Framework¹⁷ as well as the Chartered Institute of Information Security (CIISec).

As guidance, AISA points to several established and successful mechanisms employed by government agencies internationally which establish formal requirements in terms of professionalisation of the cyber security industry. For example, the US Department of Defence (DoD) 8570.01¹⁸ Manual formally recognises approved baseline industry certification levels that cyber security professionals can qualify against to certify their knowledge, skills and experience being to a rigorous standard. In the example of the US DoD 8570.01 Manual standard, all US government employees must hold a certification on the list pursuant to their role and seniority level. The certifications listed on the UD DoD 8570.01 are also currently recognised under the AS / NZS / ISO 17024 personnel accreditation¹⁹ scheme, establishing the shortlist of quality certifications that could and should qualify for consideration for a proposed Australian scheme.

RECOMMENDATIONS

- Establish an Australian scheme similar to the US DoD 8570.01 Manual that mandates approved baseline certifications that are AS / NZS / ISO 17024 accredited and are formally vetted by Government for inclusion into such a scheme.
- Align the proposed scheme to a standardised, mandated, and publicised National Cyber Security Skills Framework.
- Mandate the established scheme for Federal Government cyber security employees and work with states / territories to implement the same in their jurisdictions.
- Promote this scheme and the National Cyber Security Skills Framework for use by the private sector, academia, and industry for external alignment.

¹⁴ <https://www.cyber.gov.au/acsc/view-all-content/programs/irap>.

¹⁵ Australian Signals Directorate, 'ASD Cyber Skills Framework', <<https://www.cyber.gov.au/acsc/view-all-content/publications/asd-cyber-skills-framework>>.

¹⁶ <https://www.austcyber.com/resources/dashboards/NICE-workforce-framework>

¹⁷ <https://www.dta.gov.au/blogs/future-digital-career-pathways-aps>.

¹⁸ <https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/>

¹⁹ International Standards Organisation (ISO), 'ISO/IEC 17024:2012 Conformity Assessment – General Requirements for bodies operating certification of persons', <https://www.iso.org/standard/52993.html>.

3 - A lack of industry representation on the Department of Home Affairs Cyber Security Industry Advisory Committee.

AISA believes it is essential the voice of the cyber security industry is represented on the Committee to ensure the *2020 Cyber Security Strategy* can be successfully executed.

The Cyber Security Industry Advisory Committee,²⁰ established to assist the Department of Home Affairs in executing the *2020 Cyber Security Strategy* in October 2020, is a step that AISA welcomes. The existence of the Committee ensures that the voice of industry and the private sector can be heard by the Government.

AISA is concerned, however, that there is a profound lack of representation from major professional industry associations on the Cyber Security Industry Advisory Committee. By including the associations that can represent the views of cyber security professionals working in government, academia, and industry, this will ensure that this vital part of the cyber ecosystem is represented and heard on the Committee, and Government should consider the current situation a major missed opportunity that needs to be addressed as a matter of priority.

RECOMMENDATIONS

- Ensure that appropriate representation exists on the DHA Cyber Security Industry Advisory Committee from key cyber security, risk manager and privacy professional industry associations such as AISA, (ISC)², ISACA, and IAPP.
- Actively solicit continual and ongoing feedback from industry professionals working in the information security and privacy fields on a day-to-day basis when devising national cyber security policy.

2. Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?

AISA firmly believes that negative externalities and information and power asymmetries create a need for government action on cyber security.

The current cyber threat environment is well documented both in Australia and globally. The gravity and severity of the cyber threat situation 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. Conflating an already dire situation has been the Covid-19 pandemic that has resulted in numerous high-profile breaches and incidents have occurred within numerous Australian organisations large and small.

The latest statistics published by the Australian Governments Office of the Australian Information Commissioner (OAIC) covering the period of January to June 2021 indicate that data breaches arising from ransomware incidents increased by 24%, from 37 notifications last reporting period to 46.²¹ Further, malicious, and criminal attacks remain the leading source of data breaches, accounting for 65% of notifications. OAIC Commissioner Angelene Falk has said that the increase in ransomware incidents was cause for concern, particularly due to the difficulties in assessing

²⁰ <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/industry-advisory-committee>.

²¹ Office of the Australian Information Commissioner Australian Government 'Notifiable Data Breaches Report – January-June 2021', <<https://www.oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/Notifiable-Data-Breaches-Report-Jan-Jun-2021.pdf>>.

breaches involving ransomware. It should be noted that the July to December 2020 period showed the highest number of recorded notifications ever recorded by the OAIC.

These results are further reinforced by the *ACSC Annual Cyber Threat Report* issued by the Australian Signals Directorate in conjunction with the Australian Federal Police and the Australian Criminal Intelligence Commission.²² This report indicated 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. In fact, the report illustrated that over the period, over 1,070 cyber incidents to organisations defined by DHA as ‘critical’ were reported.

With the continuing digitisation of everything, interconnectedness, the ubiquity of social media platforms, the age of the Internet of Things (IoT), increased dependency on systems, and the erosion of privacy, the cyber threat environment is set to continue to worsen. Given this, it is almost certain that cyber security 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.

However, the multitude of threats related to cyber security are, even today, met inadequately by some Federal government departments. The *Cyber Security Strategies of Non-Corporate Commonwealth Entities* report released by ANAO in March 2021 demonstrated that numerous Federal government departments have failed to demonstrate adequate maturity to the ASD *Essential 8*, including the Department of Prime Minister and Cabinet, the Attorney-General’s Department, the Australian Trade and Investment Commission and The Department of Education, Skills and Employment.²³ Similar reports have illustrated deficiencies at a State Level, including in NSW.²⁴

Given the sheer magnitude of the negative externalities and asymmetries involved for everyday Australian individuals and organisations to protect themselves from this risk, it is imperative that the Australian Government increase both its own resilience as well as national resilience and facilitate preparedness for both the public and private sector to cyber security issues. The role of government to act as an exemplar of good cyber security practice, as a guide to what good cyber security should look like is critical. In addition, there are significant economic and social benefit to be realised by achieving cyber resiliency in Australia. It should also be noted that current advice provided by the ACSC to businesses is often technical in nature, directed exclusively at IT / security departments as the audience, and critically, it can be many weeks behind advice from the private sector at times.

RECOMMENDATIONS

- Government to lead by example in promoting strong cyber security culture, provide clear direction and demonstrate its own cyber security resiliency in addressing identified historical shortcomings.
- Government to provide clear, concise, and unambiguous standards-based advice to business and individuals as to preventative and mitigation measures that address the people, process, 3rd party supply chain and technology aspects of cyber security.
- Information and advice must be timely, inclusive and easily understood by boards and executives.

²² <https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf>

²³ <https://www.anao.gov.au/work/performance-audit/cyber-security-strategies-non-corporate-commonwealth-entities>

²⁴ <https://www.audit.nsw.gov.au/our-work/reports/managing-cyber-risks>

The current regulatory framework

3. What are the strengths and limitations of Australia's current regulatory framework for cyber security?

AISA contends that there are numerous and significant policy shortfalls and limitations with respect to Australia's aging and patchwork cyber security and privacy regulatory framework that need to be addressed.

It is often said that regulation lags technological advancement and regrettably, this is best evidenced in the cyber security realm. Specific lagging elements of the framework and recommendations include:

- The *Privacy Act 1988 (Cth)*, in its current form, is not fit for the needs of an interconnected and digital economy. AISA has made a detailed submission to the Attorney-General's Departments review of the Privacy Act 1988 and recommends that the positions taken in the submission are adopted in the future reforms of the Privacy Act.²⁵
- The *Privacy Amendment (Notifiable Data Breaches) Act 2017*²⁶ (NDB) only applies to Australian Privacy Principle (APP) entities of a certain size. However, the current nature of the digital ecosystem means that many smaller entities with equally sensitive and critical data are not covered. AISA recommends that the NDB regime be expanded to cover all APP entities.
- State and Local government is not accountable to the Commonwealth NDB regime. This has resulted in each state enacting their own NDB laws, if they have enacted any at all. AISA recommends that NDB laws be unified and a standardised NDB approach that covers all applicable entities operating in Australia be considered and implemented. This could also be pursued as part of the *Privacy Act* reforms.
- Amendment of the *Corporations Act* to ensure that directors and officers are dutifully responsible as fiduciaries for data breaches which occur.²⁷ This is an approach adopted in the State of New York through the proposed *New York Privacy Act*. Australians should not have to wait for a 'cyber Centro', where ASIC brought a civil case against Centro directors for wrongly classifying around \$2 billion of liabilities as "non-current" and failing to disclose substantial guarantees granted by Centro post-balance sheet date. AISA asks whether ASIC or another regulator do undertake a similar action in the event of a major breach.
- Future assessment of the effectiveness of the recently passed *Online Safety Act 2021* in providing protections for everyday Australians relating to image-based abuse, cyber bullying, abhorrent violent conduct.
- A lack of scope and meaningful regulatory oversight relating to cyber security for critical infrastructure. AISA notes the work currently in progress to amend the *Security of Critical Infrastructure Act 2018* and AISA has provided submissions both for the Call for Views²⁸ as well in relation to the Exposure Draft of the bill.²⁹ AISA is of the view that considering recent breaches on critical infrastructure world-wide, strong regulatory oversight is needed for critical infrastructure to ensure sector regulators can provide meaningful standards, support, oversight, and governance to sector operators. AISA notes that the Security of

²⁵ <https://www.ag.gov.au/sites/default/files/2020-12/australian-information-security-association.PDF>

²⁶ <https://www.legislation.gov.au/Details/C2017A00012>

²⁷ <https://www.itnews.com.au/news/company-directors-could-be-held-accountable-for-cyber-security-failures-567280>

²⁸ <https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-infrastructure-consultation-submissions/Submission-141-Australian-Information-Security-Association.PDF>

²⁹ <https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-infrastructure-consultation-submissions/EDS094-CISoNS-AustralianInformationSecurityAssociation.PDF>

- Critical Infrastructure (SOCl) amendments are still being finalised.³⁰
- Any new or amended cyber security or privacy legislation requires that commensurate levels of funding be provided to regulators including the Human Rights Commission and the OAIC which will enable them to enforce the legislation and remediate any harms that eventuate from breaches of legislation. Should this not be possible, the legislation should be accompanied by a second reading speech to Parliament by the Minister responsible for the legislation that commits the Government to provide specified additional funding.
 - The vast complexity of who at a federal level is responsible for cybersecurity in Australia.³¹ There is significant overlap in responsibilities which in turn creates poor accountability. This can be visible in the ANAO reports on cybersecurity preparedness.³² AISA recommends outlining clear accountability and responsibilities for cybersecurity that is enshrined in regulation and legislation.
 - A lack of professional certification scheme for cybersecurity workers. As indicated earlier in the submission, a distinct lack of professionalisation in cybersecurity is concerning, particularly given the increasingly sensitive nature of information that individuals working in cybersecurity are managing. Similar to regulated professions such as law, medicine, accounting, electricians, plumbers, and other professions, AISA forms the view that the cybersecurity workforce requires professionalisation.

RECOMMENDATIONS

- Amend the *Privacy Act 1988* to address identified shortcomings noted through the Consultation of the *Privacy Act Review*. Provide regulators responsible under the *Privacy Act* with resources required to perform their regulatory functions diligently and competently.
- As recommended in the *Privacy Act Review*, amend the NDB scheme to base the determining criteria on whether a breach needs to be notified based on the nature of the data in question, rather than revenue or entity size.
- Implement an all-encompassing NDB scheme that applies to all entities, regardless of whether they are state or federal.
- Amend the *Corporations Act* to codify directors' and officers' duties in respect to cyber security. This could include the incorporation of a fiduciary duty element.
- Review the effectiveness of the *Online Safety Act* once it is in force.
- Establish strong regulatory oversight and a mandatory standard as part of the proposed *Security of Critical Infrastructure* reforms.
- Streamline responsibility for cyber security matters at a federal level and appoint a clear and accountable body that is wholly responsible for the promulgation and adoption of cybersecurity standards and represents the 'go-to' agency for all government departments to engage with to ensure their cyber security posture is appropriate to the risk.
- Professionalisation of the cybersecurity workforce like other regulated professions such as medicine, law, accounting and the trades.

³⁰ <https://www.lexology.com/library/detail.aspx?g=d5ffe50e-94b1-4978-ac08-bc604ab336df>

³¹ Australian Cyber Security Infrastructure (v10 August 2019), Baker McKenzie, <https://www.bakermckenzie.com/-/media/files/insight/publications/2019/09/cyber_security_infrastructure_australia_chart.pdf>

³² <https://www.anao.gov.au/work/performance-audit/cyber-security-strategies-non-corporate-commonwealth-entities>

4. How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?

AISA believes that the best way to evolve clarity, coverage and enforcement of cyber security requirements will be to implement the recommendations made at Question (3).

RECOMMENDATION

Refer to Question (3) of this submission.

Governance Standards for Large Businesses

5. What is the best approach to strengthening corporate governance of cyber security risk? Why?

AISA firmly believes assigning a fiduciary duty on directors to be responsible for privacy and cyber security (as currently taking place in New York under the concept of a 'data fiduciary')³³ and amendment of the *Corporations Act* to look at the privacy of data as a fiduciary responsibility for officeholders.³⁴

Reasonable protection of personal information is critical; however, legislation should focus on the sensitivity of the personal information and the impacts and risks in the event of a data breach. A data breach can leave individuals in a vulnerable position or at a risk of serious harm and remediation should be prescribed in legislation. This positioning is discussed at length in AISA's submission to the *Privacy Act* review.³⁵ Support for individuals affected by a data breach should come from Government funded agencies. These resources should be supplemented by federal emergency services via the ACSC or the OAIC, as examples.

RECOMMENDATIONS

- Amend the *Corporations Act* to codify directors' and officers' duties in respect to cyber security. This could include the incorporation of a fiduciary duty element.
- Amend the *Privacy Act* to address identified shortcomings noted through the Consultation of the *Privacy Act Review*.
- Provide regulators responsible under the *Privacy Act* with resources required to perform their regulatory functions diligently and competently particularly with respect to supporting individuals affected by breaches of their rights under the *Privacy Act*.

³³ <https://www.gibsondunn.com/new-york-privacy-act-update-bill-out-of-committee-moves-to-full-senate/>

³⁴ <https://www.afr.com/chanticleer/directors-must-face-cyber-risks-20210310-p579i2>

³⁵ <https://www.ag.gov.au/sites/default/files/2020-12/australian-information-security-association.PDF>

6. What cyber security support, if any, should be provided to directors of small and medium companies?

AISA supports the successful work that the ACSC and OAIC have achieved thus far to provide guidance to a range of organisations and individuals. AISA believes their role in these activities should continue to be supported and funded, particularly relating to the work the ACSC and the OAIC provide to individuals and small to medium sized organisations.

AISA supports best practice guidance related to cyber security which includes:

- Cyber security advice of a general nature, such as the ACSC *Small Business Cyber Security Guide*.³⁶
- People, process, and technology related guidance, particularly the importance of using skilled, qualified, and experienced cyber security professionals such as those who hold AS/NZS ISO/IEC 17024 accredited certifications (Conformity assessment - General requirements for bodies operating certification of persons) which include certifications issued by bodies such as Cloud Security Alliance (CSA), CompTIA, ISACA, (ISC)², IAPP, and others.
- Five Safes Framework: Safe People, Safe Projects, Safe Settings, Safe Data and Safe Outputs.
 - The purpose of the model is to simplify the complex discussion around data access into a set of related but independent questions, so that each topic could be dealt with succinctly and unambiguously.
 - The framework is an internationally recognised and holistic approach to addressing strategic, privacy, security, ethical and operational risks associated with data disclosure or release that could (re)identify individuals. It takes a multi-dimensional approach to managing disclosure risk.
- OAIC issued guidance such as:
 - Guide to securing personal information and 'Reasonable Steps' to protect personal information.
 - 10 steps to undertaking a privacy impact assessment.³⁷
 - Data breach preparation and response.

AISA, the AICD and other professional associations provide a range of support to directors today in this area. The Australian Government should consider grants to support these types of associations, especially as many have been adversely impacted by the COVID-19 pandemic and these organisations are currently not supported by government. These organisations offer a rich set of guidance for directors and these efforts should be incentivised and supported. As an example, AICD and AISA have been strategic partners for several years, providing initiatives such as:

- The Australian Governance Summit
- Annual Directors update
- Cybercon – Australia's largest cyber security conference
- Cyber security hybrid events
- Content for director and member magazines
- Partnership in publications
- Roundtable series.

³⁶ <https://www.cyber.gov.au/acsc/view-all-content/publications/small-business-cyber-security-guide>

³⁷ <https://www.oaic.gov.au/privacy/guidance-and-advice/10-steps-to-undertaking-a-privacy-impact-assessment-poster/>

RECOMMENDATIONS

- Adequately fund and support bodies such as the OAIC and the ACSC into performing their missions in providing timely, meaningful, and appropriate advice and support to Australians and Australian organisations.
- Provide guidance to directors in relation to appropriate personnel accreditation / certification schemes for cyber security professionals working in their organisation such as AS / NZS / ISO / IEC 17024 and advocate for the inclusion of duly accredited individuals within the cyber security, risk management and privacy functions of organisations.
- Support initiatives and schemes operated by bodies such as AISA and the AICD that seek to educate and inform directors within small and medium businesses through the provision of grants and funding.

7. Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?

AISA believes that additional education and awareness raising initiatives for senior business leaders is required which should include small to medium sized organisations, as opposed to only larger enterprises. Directors of larger organisations should have the resources to comply, so their focus would include implementing appropriate frameworks and risk management strategies to ensure their internal controls are adequate to deliver the appropriate outcomes for their customers, other stakeholders and commensurate with their organisation's risk appetite.

Cyber security should now be an essential aspect of every senior business leader's duties. Further specific training for business leaders' compliance obligations as to cyber security risk should be provided and leaders should be encouraged to undertake this training and other professional training from AICD, AISA and other organisations on a regular basis. Prominent examples include the AICD Boards Role in Cyber Security course.³⁸

The University sector should also be encouraged by government to develop short courses or modules for directors and executives. These should be included in the various MBAs offered by the sector as mandatory units.

RECOMMENDATIONS

- Build training for executives to help them effectively deal with privacy and cyber security in their business-as-usual processes and projects.
- Expand training of today's directors to increase cyber-related coverage via grants to organisations like AICD and others that are currently equipped to deliver it to their members.
- Build the next generation of skilled ICT and cyber security directors, with specialised training targeted to today's cyber security executives who aspire to serve on boards.

³⁸ <http://aicd.companydirectors.com.au/education/courses-for-the-director/online/online-education/the-boards-role-in-cyber>.

Minimum standards for personal information

8. Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?

AISA is of the strong belief that the *Privacy Act 1988* represents the best opportunity for a general uplift of cyber security standards across Australia. AISA forms the view that cyber security represents a tenet of privacy and provisions under the *Privacy Act* should natively apply to cyber security considerations rather than being 'siloes' away from the general provisions contained in the *Privacy Act*.

AISA has made a detailed submission to the Attorney-General's Departments review of the *Privacy Act 1988* and recommends that the positions taken in the submission are adopted to facilitate this goal.³⁹

RECOMMENDATION

Implement an amended *Privacy Act 1988* in line with recommendations made by AISA through the *Privacy Act Review* process. This will ensure increased uptake and effectiveness of cyber security standards in Australia under the general protections and provisions contained within the *Privacy Act*.

9. What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?

AISA believes that the most cost-effective controls that will achieve the most impact under the code are not technical, but rather, administrative controls that stem from the implementation of better process through the better skilled and educated cyber security professionals. AISA forms the view that the professionalisation of the cyber security workforce is essential to achieve this outcome through existing global credentials.

AISA has made detailed recommendations to the Attorney-General's Departments review of the *Privacy Act 1988* in relation to this issue.⁴⁰ These positions include adopting the following international standards based both on organisational and personnel certification:

Organisational Information Privacy Certification

- ISO / IEC 27701

Organisational Information Security Certification

- ISO / IEC 27001 Family of Standards and Controls

Personnel Certification for Information Security and Information Privacy

- AS / NZS / ISO 17024 which governs the following industry certifications:
 - IAPP Certifications: CIPP/E, CIPP/US, CIPT, CIPM
 - (ISC)² Certifications: CISSP, CCSP, SSCP, CSSLP, HCISPP, CISSP-ISSMP, CISSP-ISSEP, CISSP-ISSAP
 - ISACA Certifications: CISM, CISA, CRISC, CGEIT, CPDSE
 - CompTIA Certification: Security+, CASP

³⁹ <https://www.ag.gov.au/sites/default/files/2020-12/australian-information-security-association.PDF>

⁴⁰ Ibid.

RECOMMENDATIONS

- Focus on the 'People' and 'Process' controls in cyber security. These will result in better 'Technology' outcomes.
- Adopt ISO 17024 for personnel accreditation and recognise ISO 17024 and accredited certifications within the *Privacy Act*.
- Adopt ISO 27001 for process controls and promote ISO 27001 certification for organisations to validate their cyber security strategies, processes and controls.

10. What technologies, sectors or types of data should be covered by a code under the Privacy Act to achieve the best cyber security outcomes?

AISA has made a detailed submission to the Attorney-General's Departments review of the *Privacy Act 1988* and recommends that the positions taken in the submission are adopted.⁴¹ AISA contends that more extensive details on privacy and security requirements, including in relation to information, personnel and physical security and governance, would be valuable for all sectors.

For Australian government, this detail exists in external frameworks including the Protective Security Policy Framework (PSPF),⁴² the ISM and the *ASD Essential Eight*. Most departments and agencies are already bound by the PSPF, and it is likely that the PSPF will soon be amended to require compliance with the Essential Eight. Most states have similarly adopted their own policies and standards which refer to Commonwealth or international standards. As previously noted, these harmonisation efforts should continue to allow governments and industry sectors to work together.

The Digital Transformation Agency (DTA) Certification Framework works in conjunction with a suite of other government policies and frameworks, including Australia's Foreign Investment Policy, the PSPF, and the provisions protecting Critical Infrastructure and Systems of National Significance.

The Foreign Investment Review Board (FIRB) is a non-statutory body that provides advice to the Treasurer and the Government on Australia's Foreign Investment Policy and its administration. In Australia, foreign investment is regulated by a framework that includes the *Foreign Acquisitions and Takeovers Act 1975* (FATA), the *Foreign Acquisitions and Takeovers Regulation 2015* (the Regulation) and the Foreign Investment Policy.

These should be considered for industry, all technologies, sectors, and personal information should be covered by the code. Critical sectors as outlined in the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* must be specified and aligned. These include communications; financial services and markets; data storage or processing; defence industry; higher education and research; energy; food and grocery; health care and medical; space technology; transport; and water and sewerage.

⁴¹ <https://www.ag.gov.au/sites/default/files/2020-12/australian-information-security-association.PDF>

⁴² <https://www.protectivesecurity.gov.au/>

Standards for smart devices

11. What is the best approach to strengthening the cyber security of smart devices?

ASIA believes that the principles of security by design and privacy by design coupled with guiding principles and regulations contained within an amended Privacy Act would be the best approach to strengthen the cyber security of smart devices.

RECOMMENDATIONS

- Enshrine 'security by design' and 'privacy by design' principles within an amended Privacy Act 1988.
- Establish penalties for selling unsafe IoT to consumers within the amended, mandatory Code of Practice: Securing the Internet of Things for Consumers (Code of Practice).

12. Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt for as a standard for smart devices?

AISA contends that any considered standard that seeks to promote safer technology is valuable. AISA believes that ESTI EN 303 645⁴³ represents a good IoT security standard.

While AISA would prefer to see an ISO-based standard employed, given the belief that international standards incorporate best practice, it is noted that ISO 27400 for IoT security is currently under development. It is highly likely that many of the approaches that ESTI EN 303 645 contains will be employed by ISO 27400.⁴⁴ AISA believes that while ISO 27400 would be the best standard to employ in the long term, ESTI EN 303 645 is an appropriate standard to be used in the interim. AISA also believes that the best organisational outcome in terms of overall cyber security would be to combine ISO 27400 / ESTI EN 303 645 for smart devices with ISO 27001 for the organisations overall cyber security strategy.

a. If yes, should only the top 3 requirements be mandated, or is a higher standard of security appropriate?

AISA recommends that all provisions under Section 5 of ESTI EN 303 645 be implemented. An arbitrary 'top 3' based on ESTI EN 303 645 would still leave significant shortfalls in security and introduce unnecessary vulnerabilities waiting to be exploited by cyber criminals for wider access into an IT system.

⁴³ https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

⁴⁴ <https://www.iso.org/standard/44373.html>

b. If not, what standard should be considered?

As earlier mentioned, ISO 27400 may be more suitable longer term to harmonise with global supply chains for IoT devices. However, it should be noted that prior standards development would suggest that it is likely that many of the provisions contained in ESTI EN 303 645 will be incorporated into ISO 27400. AISA also forms the view that Standards Australia can actively partake in the development of ISO 27400, potentially to develop an Australian standard based on ESTI EN 303 645.

RECOMMENDATIONS

- Commission Standards Australia to develop an Australian standard based on ESTI EN 303 645 in the short to medium term as a smart device security and privacy standard in Australia.
- Standards Australia could then seek international acceptance of the Australian Standard, possibly for inclusion into the proposed ISO 27400 standard.
- Evaluate the final release of ISO 27400 with a medium to long term view of incorporating that standard for smart device security and privacy.
- Promote ISO 27400 and ISO 27001 as appropriate standards for smart devices as well as cyber security more broadly.

13. Would you be willing to voluntarily remove smart products from your marketplace that do not comply with a security standard?

AISA believes that the regulatory burden on small to medium sized retailers to voluntarily remove smart products from their marketplace which do not meet a security standard will be onerous and unfair. Reasons for this include:

- Most retailers will fail to understand what meets or does not meet the standard unless the product is accompanied by an appropriate labelling scheme.
- Standards evolve and change. Consequently, some products that are compliant today may not be in the future. This will invariably add cost and risk to retailers which will need to be absorbed or most likely passed on to the consumer.
- Non-compliant products sold through non-traditional online retailers (e.g. eBay or Alibaba) will be a cheaper option for the public, thereby circumventing the objective of protecting consumers. In addition, this competition with non-compliant products also removes any balance or incentives for traditional retail outlets based in Australia to voluntarily remove products from the marketplace.
- A scheme of this nature would be dependent on clear standardised labelling by manufacturers to make it easier for consumers, retailers, and regulators to monitor and make choices.

Larger digital platforms like Amazon, Apple, Facebook, Microsoft, and Google and large retailers should be able to filter these unsafe products as they have the resources and capabilities to do so. This will inadvertently apply a disadvantage to small and medium retailers without the resources.

RECOMMENDATIONS

AISA does not recommend a voluntary scheme to remove smart products from the market that do not comply with a security standard. Further:

- If a scheme is introduced by the Australian Government, it needs to be mandatory across all large retail or digital platforms and voluntary for small to medium sized entities. It also needs to be aligned with a mandatory labelling scheme to enable retailers, consumers, and regulators / enforcers to monitor and make decisions. Under the scheme not all products need to be listed or labelled accordingly to a specific standard, but only those listed on a schedule of products.
- Under a mandatory scheme a credible authority also needs to have the powers and resources to force redress and enforcement (e.g., the ACCC) to protect consumers. Retailers also need protections to allow inventory to be sold when standards do change, ensuring there is a period of transition to any new higher standard, preventing retailers having to bear the burden of losses with outdated stock.
- Legislative models and rules relating to products meeting specific standards already existing in Australia. For example, plumbing products installed in Australian homes from a specific schedule of products must bear the trust mark called WaterMark and are approved for installation / use. Products listed on the schedule of products which do not bear the WaterMark are illegal to install and consumers are advised to report those products in the Australian marketplace.
- Product recalls must also be considered under a scheme where products must conform to a standard. These recalls would occur if the product was found to cause damage or loss of life to consumers in instances where it fails to meet the standard. This also assumes that an enforcement body is funded and capable of testing compliance to the Australian standard and has the resources to receive public complaints or investigate product / manufacturing failures. This would be no different to existing controls within the Australian market where products are certified to meet a standard by fail to do so (e.g., electrical wire imported from China that does not meet Australian electrical standards due to a product fault⁴²)

⁴⁵ <https://esv.vic.gov.au/technical-information/safety-alerts-and-product-recalls/infinity-and-olsent-cable/infinity-olsent-cable-recall-consumers/>

15. Is a standard for smart devices likely to have unintended consequences on the Australian market?

Unfortunately, Australia manufactures little by way of smart devices at this current time. Any obligations on the sale or manufacture of smart devices would be imparted primarily on the supply chain, primarily based overseas, which would place a positive obligation on importers and retailers to ensure their supply chain partners comply with Australian requirements, the same other products imported into Australia require compliance as covered by other standards or trust marks (e.g., WaterMark⁴⁶).

Enforcing a standard on smart devices will likely have unintended consequences, initially, or at least until those standards are adopted by other major markets such as the USA, Europe or UK. These consequences may be in the form of:

- higher prices paid by Australian consumer;
- the lack of product availability in the Australian market as the cost burden for some manufacturers may be too high, thereby forcing consumers to shop online and import the product from other global retailers;
- barrier for inbound start-up / innovation organisations establishing businesses in Australia.

A possible consequence may be the emergence and development of local Australian innovation start-ups specifically designing 'secure by design' smart products for the Australian market, with a view for global expansion later as other countries follow the Australian example. These entities could also benefit from schemes that support Australian organisations seeking to export overseas.

If Australia were to follow efforts such as the State of California as a first mover in this area,⁴⁷ it would signal to the market a need for improved products and standards associated with smart devices. However, without alignment with other countries and markets, the Australian Government should expect potential negative consequences for Australian consumers and some Australian businesses.

⁴⁶ <https://watermark.abcb.gov.au/consumers/what-watermark>

⁴⁷ SB-327 Information Privacy: Connected Devices, California Legislative Information, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

Labelling for smart devices

16. What is the best approach to encouraging consumers to purchase secure smart devices?

AISA believes further analysis to test different labelling schemes with various segments of the Australian public (e.g., technical people through to non-technical individuals) is needed, based on our Member Survey.

Labelling products is known to drive consumer purchasing decisions and examples can be seen from vehicle fuel consumption labels through to energy rating stars. Over the last two years, AISA has conducted research in this space to determine what consumers and specifically cyber security professionals view as the best solution regarding labelling IoT / smart devices.

Several existing labelling solutions existing across some product segments for Australian consumers. These range from:

- **Energy / Water efficiency rating** – used to drive consumer choices to buy more efficient devices and subsequently encourage manufacturers to produce more efficient devices (as driven by consumer demands). The rating of a device is at the time of certification for that product, however the device over time will obtain a lower efficiency rating if the manufacture puts the same device through the rating process. Consequently, whitegoods⁴⁸ purchased by consumers at one point which are ‘5 stars’, might become ‘2 stars’ over a period (e.g., 10 years). This will drive several positive outcomes:
 - Drives consumer demand for higher efficiency devices (due to the operational cost savings).
 - Encourages manufacturers to produce devices that are increasingly efficient as the standard behind the rating system increases.
 - Enables manufacturers to differentiate from competitors in the market (e.g. driving efficiency which is the intention of the rating systems).
 - Ensures retailers are not left with stock that may be viewed by the consumer as expired or outdated.
- **Nutrition labelling system** – this is a more complex labelling scheme which distils many common attributes of products sought by consumers. While complex, it does provide consumers in the know (e.g. who have an understanding about calories, nutrition etc..) with the information they seek to make informed choices. To be effective, this type of labelling requires consume education with regards to cyber security to help consumers identify what is good and what is bad. The advantage of this type of labelling is the amount of information that can be conveyed to consumers which might be useful when communicating if their data remains in Australia, how often the product is updated, if it has automatic security updates, if personal details are captured and stored on the device or pushed to the cloud etc...).
- **Trust Mark**- this type of labelling scheme is very simplistic and can be used to convey trusted products or approved products that meet standards (e.g. WaterMark). It can convey information quickly due to the simplistic nature, but also lacks the detail needed for smart devices. Some have suggested using an expiry date with the trust mark to convey when a

⁴⁸ <https://www.energyrating.gov.au/>

device is no-longer expected to be secure, however this approach is not advised as a products ability to be compromised is not time bound. In addition, just because a product ceases to receive updates from the manufacturer does not mean it is obsolete or more insecure. The usage and risk tolerance of the user is the factor that determines if the smart device is a threat to the consumer.

Key disadvantages of using a best before or secured by expiry date are:

- it would render products obsolete when they are not;
 - it creates a false sense of security and an incident linked to a product which is label as secure devalues the labelling scheme;
 - it would disincentivise retailers to keep stock which would decline in value to the consumer (e.g. considering milk, most people will prefer to buy the carton with the longer shelf life) and;
 - it exacerbates the problem of e-waste with people disposing of products that are past their artificial secure date.
- **Informative labels** – This includes devices such as the tyre feature label for vehicles, which can be used to convey a limited set of key attributes visually to consumers. This enables consumers to balance their product choices on a limited set of key attributes. The biggest objective would be determining what are the four or so key attributes that reflect key considerations by consumers that allows them to make an informed choice.

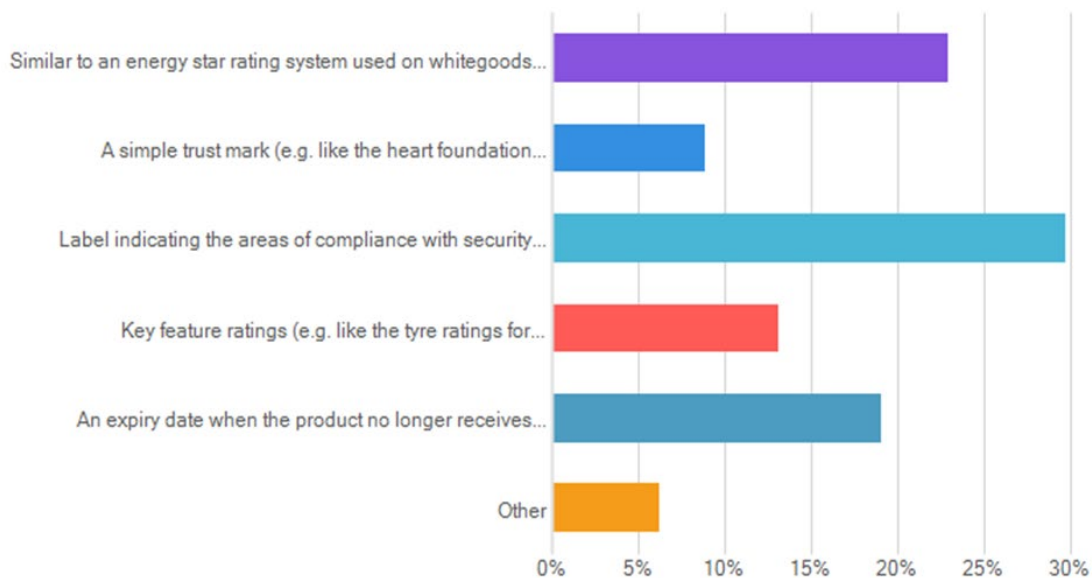


Examples of common consumer labels

AISA research has illustrated the following preference for labelling smart devices:

- An Energy Star style rating system used on whitegoods (e.g., 5 stars)- 23.0%
- A Trust Mark (e.g., the Heart Foundation 'tick')- 8.9%
- Label indicating the areas of compliance with security standard or code (e.g., a nutrition label on food)- 29.7%
- Key feature ratings (e.g., tyre ratings for noise, handling and fuel economy) - 13.1%
- An expiry date when the product no longer receives security updates (e.g., a use by / best before date)- 19.0%
- Other - 6.2%

According to the survey, approximately one-third (29.7%) of the AISA community prefers a label such as a food nutrition table, closely followed by a star rating system (23%) and a label with an expiry date as the third highest preference (19%). Least popular is the trust mark and key feature ratings.



AISA conducted additional research which specifically targeted IoT devices, as opposed to the broader description of “Smart Devices”. This research focused on the four options of using a system like energy rating, trust mark, nutrition style and key feature ratings. This research demonstrated an overwhelming level of support for the energy star rating type of label (37.4%), followed by labelling like food nutrition tables (28.6%) with key feature a third preference (25.2%). The least desired was a simple trust mark, with only 3.4%.

RECOMMENDATIONS

- Further analysis to test different labelling schemes with various segments of the Australian public (e.g., technical people through to non-technical individuals).
- If a labelling scheme is selected without further analysis and consideration, the overwhelming popularity based on studies conducted by AISA are nutrition style labelling listing how a product meets specific defined requirements allowing consumers to make comparisons across manufacturers / products or a simple energy start rating type system.
- It is plausible that technology savvy users prefer a labelling system with more details while general non-technical consumer may prefer a simple star rating system to enable quick purchasing decisions.
- AISA did conduct some purchasing decision research to determine how product pricing with a label impacted purchasing decisions and found that labelling did assist to drive purchasing decisions even if the product with the label was more expensive, indicating that a label of some type increased consumer purchasing confidence.

17. Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?

A combination of appropriate labelling and standards for smart devices would be a practical and effective approach as this type of system has already been demonstrated to be effective in electrical and plumbing products.

However, it does require investment from the Government to ensure a relevant authority with the appropriate powers to address consumer redress, recalls and fines for breaches. It is important however that the adoption of standards appropriate for the Australian marketplace be defined by Standards Australia. Standards Australia is best placed to take an existing international standard and adapt it for the Australian market.

RECOMMENDATIONS

- If the Australian government wants to introduce labelling or a standard, they must both be introduced together or not at all.
- Have the standard defined and managed by Standards Australia.
- Recognise that additional investment is required to educate the market and manufacturers.
- Create an appropriate authority for overseeing the sector to be empowered through legislation, be funded, and resourced appropriately.

18. Is there likely to be sufficient industry uptake of a voluntary label for smart devices? Why or why not? a. If so, which existing labelling scheme should Australia seek to follow?

The voluntary 'IoT Code of Conduct' introduced by the Government has been ineffective, with little to no uptake by the industry. AISA contends that the incentives either in terms of consumer choice or criminal / civil actions are too low. As a result, manufacturers are ignoring the Code.

The security of smart devices is an afterthought by most consumers. Security is not the primary function of the device they are purchasing. While technology savvy individuals are more likely to investigate and assess the security of a smart device, this is often difficult to do with the manufacturer not disclosing standards they might be compliant with, how and where data collected by the device is stored or other security features of the smart device. Technology savvy individuals often resort to online videos produced by review sites or through discussion with other concerned consumers.

For a scheme to be effective, and to ensure equity in the market, a scheme needs to be mandatory. It is also important to clearly articulate the purpose of such a scheme to ensure it is recognised and understood. Is the proposed scheme to reduce liability, save lives, prevent injury, protect infrastructure, improve business cyber resilience? The motivation and objective is essential in determining the type of scheme that is introduced. In addition, is the target audience consumers, enterprises, small to medium sized enterprises? Depending on the target audience, this will radically change the scheme, funding and oversight levels.

Lastly, as we have learned from the *Privacy Act*, without sufficient penalties, organisations are likely to willingly or unwillingly ignore any voluntary code. It has been demonstrated over many years that digital platforms willingly ignore consumers and only pay attention when strong punitive damages are introduced.

RECOMMENDATIONS

- Clearly specify the intended target audience and the motivation for the scheme (e.g., the behaviour the Government wants to drive, and the risks to mitigate) as a one-size fits all may not be suitable, resulting in a scheme that when implemented is not fit for purpose and has poor outcomes for organisations, manufactures and consumers.
- If the Government introduces a scheme, ensure it is adequately regulated, funded, resourced, and enforced.

19. Would a security expiry date label be most appropriate for a mandatory labelling scheme for smart devices? Why or why not?

AISA believes there could be some value in “best if used by” or “security not assured after” date if manufacturers are willing to stand by these dates for supporting their products and these dates are combined with other measures, such as mandatory security standards and product recalls. A mandatory expiry date is not likely to be effective, though.

Overall, there is a balance in terms of complexity. Recall that most Australians are not technically savvy. If a device meets a security standard which incorporates regular updates on software, then an expiry date should only appear once a piece of technology has become deprecated and is no longer supported, which most consumer electronic products is between three and seven years. If a mandatory period in terms of vendor support could be instigated (for example, three years past end of sale), this may drive consumer behaviour to dispose of products which are still acceptable to use. Also, not all vendors will have consistent end of life (EOL) programs.

A vulnerability in a product is not defined by an expiry date, and as such a scheme would drive an increase in e-waste and the misconception that a device is safe and secure, when in reality a vulnerability may be discovered that compromises the device even before a user has purchased the device and updates may not be possible. Some systems / devices are designed to exist in an environment for more than three years. This is very common in sectors like utility providers where some devices could be in use for over 30 years. Other smart devices (e.g., Automatic Teller Machines) use outdated operating systems as the vendors who produce them do not support the latest operating system given the machines are often reliant on a 3rd party (i.e., they do not make the underlying operating system, but build applications that sit on that operating system from a point in time, which often break with operating system updates).

Another misconception with using an expiry date is that manufacturers have a well-defined and planned expiry dates or EOL dates for their products. This naïve misconception misses the fundamental point of EOL which is used by vendors to increase company sales by forcing consumers to move to a new product periodically or to reduce their internal costs of needing to maintain past versions of a product with limited product development resources (i.e., people and funds). The rate of change that occurs in the market, due to competition between manufacturer to capture greater market share means the real EOL for some products is less than three years, while other products in different sectors might be 10 years as the pace of change is slower.

RECOMMENDATION

Do not introduce a security expiry date label as it will drive e-waste and create a false sense of security for consumers. It would be far better to have a more comprehensive label for savvy consumers or an energy star rating style system which could have a “tested by date”.

20. Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?

Mobile/smart devices are computers in their own right – carrying even more sensitive details including geolocation and health data. As such, AISA contends that such devices should be covered under a mandatory labelling scheme.

RECOMMENDATION

If a mandatory labelling scheme is introduced, it should be across all smart devices that represent a risk to organisations or consumers. This risk should be assessed using a device class scheme which considers the following aspects: location of manufacture (e.g. overseas in a trusted country), type of data collected stored or transmitted by the device (if that data is not encrypted), if the device stores data in the cloud (and where geographically), if the device can be updated / patched, if the device has built in minimum security features that are enabled by default etc...

21. Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?

AISA does not believe it would be beneficial to label smart devices both digitally and physically. There may be concerns with digital labelling. Consider the digital identification of a smart device from a privacy perspective. A physical label on the box should suffice assuming the label represents conformity to a rigorous and respected standard that will in fact deliver outcomes for security.

However, as an example, consider the International Mobile Equipment Identity (IMEI), a 15-digit number unique to each device which represents a mobile phone’s fingerprint. Phone carriers and manufacturers share IMEI numbers to enable tracking of smartphones that may be stolen or compromised. These numbers effectively become an identity number for an individual and therefore need to be protected for privacy purposes. Digital labelling could, similarly, be used for such a purpose, representing a barrier to consumer acceptance.

RECOMMENDATION

It would be simpler and more effective to only use physical labelling that conforms to a defined standard for consumers and ensures equity in the market. This also dispels any myth of digital labels being used to track a device’s usage.

Responsible disclosure policies

22. Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?

AISA forms the view that voluntary guidance rarely works when implementing responsible disclosure policies, given different parts of the business sector operate at varying levels of capability and maturity. This variance creates inequality and complexities which can inadvertently impact businesses who are less mature.

AISA is of the belief that rather than introducing additional complexity for businesses with additional legislation, it would be far better to leverage existing legislation, which primarily consists of the *Privacy Act*. AISA has submitted a detailed response to the Privacy Act Review⁴⁹ and considers that the recommendations made in that submission will assist in implementing a responsible disclosure policy.

RECOMMENDATION

AISA strongly recommends mandatory guidance based on the extent to which information is sensitive and disclosed (in line with *Privacy Act* amendments as per AISA *Privacy Act Review* submission).

Health checks for small businesses

23. Would a cyber security health check program improve Australia's cyber security? If not, what other approach could be taken to improve supply chain management for small businesses?

AISA believes it is dependent on the nature of the program and what outcomes are desired. A poorly crafted program could offer increased business cost with limited benefit while wasting public money. Under the 2016 Cyber Security Strategy, the Cyber Security Small Business Program⁵⁰ grant involved CREST certified partners performing penetration and vulnerability testing of SMEs. This program was a failure which resulted in no benefit to the SME sector, given the lack of knowledge within the SME community around how to leverage a penetration / vulnerability test results and understand the interpretation and recommendations. AISA contends that SME's, instead, would have benefited from a consultancy approach which educated the SME about cyber security threats to their business (e.g. ransomware, Business Email Compromise etc..) and assessed the SMEs capability and maturity to becoming cyber resilient. An outcome would then be a step-by-step plan at a pace the SME can cope with from a time, price, and resource perspective to improve their cyber security posture.

To use an analogy, an increased emphasis should be placed on making the roads and the cars safe and then the driver. AISA believes too much of the responsibilities have been placed on technology users' safe use versus the on manufactures to sell safe technology.

⁴⁹ <https://www.ag.gov.au/sites/default/files/2020-12/australian-information-security-association.PDF>

⁵⁰ <https://blog.compliancecouncil.com.au/blog/australian-government-to-fund-the-ethical-hacking-of-small-businesses>

As to the users of technology in small business, any assurance program needs to be designed to be suitable to the business and resilience objectives and appropriate to the capability of the organisations. Further, these programs should be placed on the hands of other small business versus the government to provide these assurance services. AISA points out that any 'cyber security checks' are a point in time check performed in an environment which can change quickly in the context of cyber security. Subsequent acts or omissions will alter an organisations cyber posture and having a cyber check may in fact result in complacency for organisations that pass those point in time checks. In line with industry best practice, AISA recommends that any such checks need to be scheduled on a regular and recurring basis.


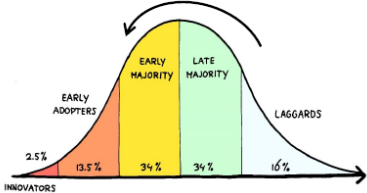
RECOMMENDATIONS

- Subsidised internships / placements of cyber security tertiary students (TAFE and University) to enable the next generation of the workforce to access hands on experience under the guidance of both industry and tertiary education providers. This also provides Small and Medium Enterprises (SMEs) with access to resources and talent to assist them. Some tertiary programs have a free placement program (typically students part way through their course) and a paid internship program in the range of \$890 ex GST per week (this typically covers students who are about to graduate). Both schemes should be supported and leveraged for SMEs. This would however require the coordination across the tertiary sector, possibly accreditation of providers and education in the SME community that these services exist.
- Reduced University course fees for courses that cover cyber security (both undergraduate and postgraduate) to rapidly increase the number of potential students studying in this field. This would create a pipeline of talent businesses can access over the next three to five years and stabilise professional salaries for cyber security professionals allowing business to access resources as opposed to being priced out of the market for skills / resources.
- Encourage universities to develop programs in conjunction with industry partners to services SMEs to improve cyber security resilience. An example of this is the recent partnership between the Victorian Government and Deakin University (DISH program focused on SME services delivered by students under the guidance of industry partners like NAB, PwC, CPA Australia, AISA and others).
- Subsidising IT and cyber security workers in Australia to attain some clearly defined internationally recognised industry cyber certifications for those professionals to better achieve continuous cyber outcomes that will deliver long term benefit for their existing organisation and the sector. A starting place may be AS / NZS / ISO 17024 accredited certifications and/or certifications defined by the US DoD Approved 8570 Baseline Certifications

24. Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?

Small businesses will only benefit from a health check program if the business understands the value of cyber security and has the right business model, attitude, and mindset towards addressing digital risks to their business. Hence, the success of such a program hinges on awareness and education first and then a level of capability and maturity. Simply speaking, it would be a waste of public money to fund health checks that are not aligned to the operational and business needs of small business.

To provide some context, the current profile of SME's in Australia can be viewed via the following 'SME Profile on a Page', provided by Debra Bordignon, Director of Deakin University's Digital Innovation for SME Hub (DISH⁵¹).

<p>2.39m of 2.40m businesses are SME</p> <p>87.4% less than 5 people 10 % 5 – 19 people 2.4% 20 – 199 people 0.2% 200+ people</p>	<p>Innovation & entrepreneurship</p> <p>85% of innovation activity is SME generated</p> <p>40% of SME's explore innovation opportunities</p> <p>Uplifting performance in – sales, profits, employment, digital investment, productivity</p> <p>BUT, R&D is not prevalent</p> <p>Just 13% of SME's invest in R&D</p> <p>And only 3% of SME's source support from the tertiary sector</p>	<p>70% are family owned</p> <p>32 yrs av. business age 55 yrs av. CEO age 35% women owners 81% owners retiring soon 41% passing along to family</p> <p><i>Top issues – communication, innovation, liquidity, capital, structure, gender equity, skills</i></p>
<p>From farm to plate and the roof over our heads - SME's are comprised of...</p> <p>10% farming, forestry, fishing 4% manufacturing 18% distribution 18% construction 31% business services 18% household services 0.4% mining</p> <p></p>	<p>Ramping up innovation</p>  <p><i>innovation appetite must shift left</i> <i>innovation cycles must accelerate</i></p>	<p>SME's are our regional fabric</p> <p>Dominate the regional economies of Victoria, NSW, WA and NT in particular</p> <p>The impacts of failure are felt broadly across rural communities</p> <p>SME survival rate is far lower than large enterprises</p>

While it is sometimes said that cyber security is top of mind for SMEs, the reality is some may be concerned or aware about cyber security as a peripheral issue, however, most are dealing with top operational issues such as communication, innovation, liquidity, capital, their business structure, gender equality and tapping into appropriate skills / resources. With the average age of a family-owned SME CEO being 55 years, many of these CEO's are more concerned with passing on the business to family or retiring, especially in a pandemic environment, than an issue such as cyber security, an issue they cannot see affecting them directly until it does.

With this in mind, any proposed health check services would either need to be free, or close to free, and will need to be specifically catered for the business or segment. Previously run government grants in this area have failed to make an impact. This is because the target market saw little to no value in the offering; the providers to deliver the service have been limited to a handful of approved providers; the experience by the SME has been poor; the SME has been too time constrained to consider the service accessing the service has been difficult in terms of time and complex paperwork; or a combination of all these.

⁵¹ <https://www.deakin.edu.au/research/research-partnerships/the-dish>

RECOMMENDATIONS

- The provision of subsidies for small business as described at Q(23) for workers in organisations to upskill and certify in cyber security.
- Better analysis of the SME sector is required as key issues for the sector are not cyber security during this pandemic.
- Pilot with existing infrastructure (e.g. DISH) to help determine what works and does not work for regional and metro SMEs. If the pilot is successful, consider expanding in each state / territory with a combination of partners (e.g. key associations, a local university and associated industry partners) to replicate the DISH model.

25. If there anything else we should consider in the design of a health check program?

Small businesses are accustomed to managing several existing regulatory risks such as OHS and fair work arrangements. In a similar vein, cyber risk also needs to be considered as part and parcel of operating a business in the digital age.

AISA is of the view that any prospective health check programs for small business should be performed by consultative by nature, with those consultations performed by a certified cyber security professional who has the appropriate skills and holds a current industry certification such as an AS / NZS / ISO 17024 defined accreditation. Such a professional should also demonstrate an understanding of the SME market. In ensuring that a cyber security professional is skilled, experienced, and qualified, that person can:

- provide the necessary and appropriate cyber and privacy guidance to organisations using best practice and industry-approved guidance, such as guidance published by the Australian Cyber Security Centre (ACSC).
- provide the facilities for organisations to develop their cyber resilience through better education, knowledge, and certification.

Complementary to the above could be to deliver a business health check in partnership with the University sector, similar to the concept of university-run community legal centres for law. This would reduce the commercial cost of delivering the service, help to educate and build the next generation of skilled workers (hence more accessible resources in the market) and would leverage university infrastructure that already exists in partnership with industry.

RECOMMENDATIONS

- Develop an Essential Eight specifically for SMEs (e.g. SME E8) that considers cloud based services, developing a resilient culture and simple controls that can be practically implemented (e.g. not whitelisting applications). The SME E8 must also be supplemented by awareness programs to drive behavioural change.
- Increase messaging to the small business sector that cyber risk is an area of concern which requires positive action on the part of the small business owner.
- Ensure that any health check program for small business, whether it be subsidised or paid by the business, be performed by a duly accredited and certified individual who holds an industry-recognised AS / NZS / ISO 17024 accreditation and is able to translate technology issues into business risk language the SME can understand.
- Leverage existing associations to work with industry partners and the University sector to deliver the service, reducing the cost to both SMEs and the use of public money.

Clear legal remedies for consumers

26. What issues have arisen to demonstrate any gaps in the Australian Consumer Law in terms of its application to digital products and cyber security risk?

AISA forms the view that the rights of the consumer in relation to digital products and cyber security risk should be paramount. AISA believes that a strong continuation of the application of the Australian Consumer Law is vital to ensure that confidence in digital products and related cyber security concerns is maximised.

Related to Consumer Law provisions, AISA has advocated for stronger measures to be incorporated within the *Privacy Act 1988* as per the AISA submission made to the Privacy Act Review.⁵²

27. Are the reforms already being considered to protect consumers online through the Privacy Act 1988 and the Australian Consumer Law sufficient for cyber security? What other action should the Government consider, if any?

AISA has made a detailed submission to the Attorney-General's Departments review of the *Privacy Act 1988* and recommends that the positions taken in the submission are adopted.⁵³ AISA contends that more extensive details on privacy and security requirements, including in relation to information, personnel and physical security and governance, would be valuable for all sectors.

As of the time of writing, AISA is unaware of any formalised recommendations derived from the Privacy Act Review process.⁵⁴

⁵² <https://www.ag.gov.au/sites/default/files/2020-12/australian-information-security-association.PDF>

⁵⁴ <https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988>. As of November 2020, no updates have been issued.

RECOMMENDATIONS

- Refer to the AISA submission to the *Privacy Act Review*.
- Consider amendments to s 50, ss 51-64A of the Australian Consumer Law to recognise the fundamental rights to privacy Australian consumers should enjoy particularly in the digital era.

Other issues

28. What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights consumers?

AISA believes that people are the most important aspect of cyber security and almost all privacy and cyber security issues and risks will be solved by addressing the 'people' element of cyber security. By solving the 'people' element, the 'process' element will be better managed, resulting in far stronger 'technology' outcomes.

Consider that directors, executives, and organisation systems users may not have sufficient training and awareness in cyber security and privacy. This lack of understanding drives resourcing issues internally, where it is often the case that security and privacy work is incorporated as an additional business-as-usual task on top of their main jobs of many of their staff. In turn, this drives a 'best effort' approach which often sees the cyber posture of an organisation fail, resulting in the breaches we see in the news every day. This eventuates in privacy loss, harm to consumers through compromise of their personal data and significant financial harm.

It is a simple fact that front-line workers operating in the cyber security and privacy space need better training, skills development and accreditation. Better qualified people will result in better process resulting in better outcomes for technology, security and privacy. The skills shortage of cyber security personnel is well known and well researched. Compounding this, the people who work in the industry are often under skilled, over worked and not supported by boards and executives.

AISA is also cognisant of the fact that there is significant ambiguity in terms of career paths and how university education, on the job work experience, vendor accreditation and industry certification fit together to ensure a professional is knowledgeable, skilled, experienced, and qualified to protect Australians. AISA forms the view that a clearly defined skills and career pathway that incorporates all these elements is crucial into professionalising the industry.

Ransomware

53% of directors, executives and cyber security professionals support making ransomware payments illegal in Australia, with only 26% not supporting making payments illegal.

AISA believes making ransomware payments illegal in Australia will result in Australian businesses and consumers becoming less of an attractive target by criminal syndicates or hostile foreign governments.

Authors

About the Lead Authors

Tony Vizza – AISA Board Director

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



Tony is a Global Advocacy Director for (ISC)², a Cyber Security Ambassador for the NSW Government, a member of the Cyber Security Industry Advisory Committee 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, the co-chair of the (ISC)² Asia-Pacific Advisory Council and has provided expert services to the United States Government Department of Energy (DoE), 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 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, Bengaluru in India. Tony is currently studying 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.

Damien Manuel – AISA Board Director and Industry Professor / Director of Deakin’s Centre for Cyber Security Research and Innovation (CSRI)

Damien Manuel is the Industry Professor and Director of Deakin's Centre for Cyber Security Research & Innovation and is the Chairperson of the Australian Information Security Association (AISA), a not-for profit organisation which aims to improve Cyber Security in Australia at a Government, Industry and Community level.



In his former role as the Chief Information Security Officer (CISO) for Symantec Australia and New Zealand, Damien worked with senior executives in the region to align security architectures to industry best practices. Damien also worked as a senior information security governance manager and later as an enterprise IT and security risk manager at National Australia Bank (NAB), where he was responsible for managing the bank’s information security standard globally. He also held senior roles at RSA, Telstra, Ericsson and Melbourne IT and was on the board of the Oceania Cyber Security Centre (OCSC).

Damien is currently on CompTIA’s Executive Advisory Committee in the USA, the Victorian Ombudsman’s Audit and Risk Committee, the board of RSA Australia, the chair of Standards Australia’s Standards development committee for cyber security and privacy, the chair of the ATN Cyber Committee and helps mentor entrepreneurs through CyRise, Australia’s only cyber security startup accelerator.

Damien has supported CompTIA for over 18 years through the development of CompTIA Server+, CompTIA Network+, CompTIA Security+ and the CompTIA Advanced Security Practitioner certification. Damien’s passion for making a difference motivated him to establish Information Technology community resource centres to improve literacy and skills in impoverished and disadvantaged communities in Kenya, Laos, Uganda and Cambodia.

Underpinning his over 25 years of experience is a diverse educational grounding ranging from the highest security, audit and governance certifications complemented by an Executive MBA with an international business focus. Damien also has a background in genetic engineering and is passionate about science. He has spoken on a number of podcasts (including with Dr Karl), conference keynotes internationally and locally, radio and TV appearances.

Michael Trovato – AISA Board Director and Managing Director & Lead Security Advisor of IIS and Research Director ISACA Melbourne Chapter

Mike Trovato is a cyber security and technology risk advisor to boards, board risk committees, and executive management. He focuses on assisting key stakeholders with understanding the obligations and outcomes of effective privacy and cyber security. This includes solving an organisation's issues with respect to regulatory, industry, and company policy compliance and to protect what matters most in terms of availability, loss of value, regulatory sanctions, or brand and reputation impacts balanced with investment.



Mike is ICG's Global Cyber Practice Leader. Prior to joining IIS, he was the Founder and Managing Partner of Cyber Risk Advisors. Before then, he was Asia Pacific, Oceania and FSO Lead Partner EY Cyber Security; GM Technology Risk and Security for NAB Group; a Partner within Information Risk Management at KPMG in New York and has held financial services industry roles at Salomon Brothers and MasterCard International.

Mike is a Graduate of the Australian Institute of Company Directors (GAICD), Member Australian Information Security Association (AISA), an AISA Board Member, ISACA Melbourne Chapter Board Member, and Member of National Standing Committee on Digital Trade.

Mike's professional credentials include being a Certified Information Systems Manager (CISM); Certified Data Privacy Solutions Engineer (CDPSE); Certified Information Systems Auditor (CISA); and PCI DSS Qualified Security Assessor (QSA). He is also a member of the International Association of Privacy Professionals (IAPP) and is an ICG Accredited Professional. He has an MBA, Accounting and Finance and BS, Management Science, Computer Science, and Psychology.

Mike is the co-author of **The New Governance of Data and Privacy: Moving from compliance to performance**, Australian Institute of Company Directors, November 2018.