Australian Information Security Association

Hon Peter Dutton, MP
Minister for Home Affairs
Australia's 2020 Cyber Security Strategy
Australian Government, Department of Home Affairs

8 November, 2019

Dear Minister,

Thank you for the opportunity to provide input to Australia's 2020 Cyber Security Strategy – A call for views.

The Australian Information Security Association (AISA), the peak body representing the nation's cyber-security sector, supports the Department of Home Affair's intention to review and produce - in consultation with the community, industry and academia - an updated and more relevant cyber-security strategy that has meaningful objectives, can easily be assessed on a yearly basis and that provides better cyber resilience for all Australians. AISA is a not-for-profit charity, established 20 years ago with the mission of educating and helping the community, industry and government to be safe online.

AISA's membership is broad and extensive and includes board directors and C-Level executives through to highly technical professionals and the next generation of the cyber-security workforce. AISA has strategic partnerships with a range of organisations and other associations to help bring together the skills required to protect Australia. Some of these partnerships include the Australian Institute of Company Directors, ASPI, Crime Stoppers, Risk Management Institute of Australia and a majority of Australia's University and TAFE sector.

AISA's annual national conference, the Australian Cyber Conference, is the largest and best-regarded event on the Australian cyber calendar, with Cyber Week and Stay Safe Online anchored around AISA's conference. This year the conference was attended by more than 3600 delegates from 24 countries.

In late October 2019, AISA surveyed its more than 6000 individual and corporate members. Their responses have guided our response to the questions posed by Government.

Yours sincerely

Alexander Hoffmann
Board Member (and on behalf of the AISA members and board)

Australian Information Security Association
ABN: 181 719 35 959
Level 8/ 65 York Street, SYDNEY, NSW, 2000
Phone: 02 8076 6012 Email: admin@aisa.org.au Web: www.aisa.org.au

1. What is your view of the cyber threat environment? What threats should government be focusing on?

As we become increasingly dependent on technology and more continuously connected online, the seriousness and impacts of disruptions, breaches and cyber attacks to the Australian economy and society exponentially increase. In AISA's survey of members, **62 per cent** of respondents had experienced an attack and **76 per cent** knew someone who had been impacted by cyber crime. When the 2016 strategy was launched, 1 in 4 Australians was impacted by cyber crime. The situation has deteriorated to the point where 1 in 3 Australians is now impacted by cyber crime, indicating that as a country we are losing the battle to protect businesses, services and the community.

On a scale of 1-10, with 10 being extremely high and 1 being very low, industry experts rated the current cyber threat level as **8** (on the extremely high end) for**:**

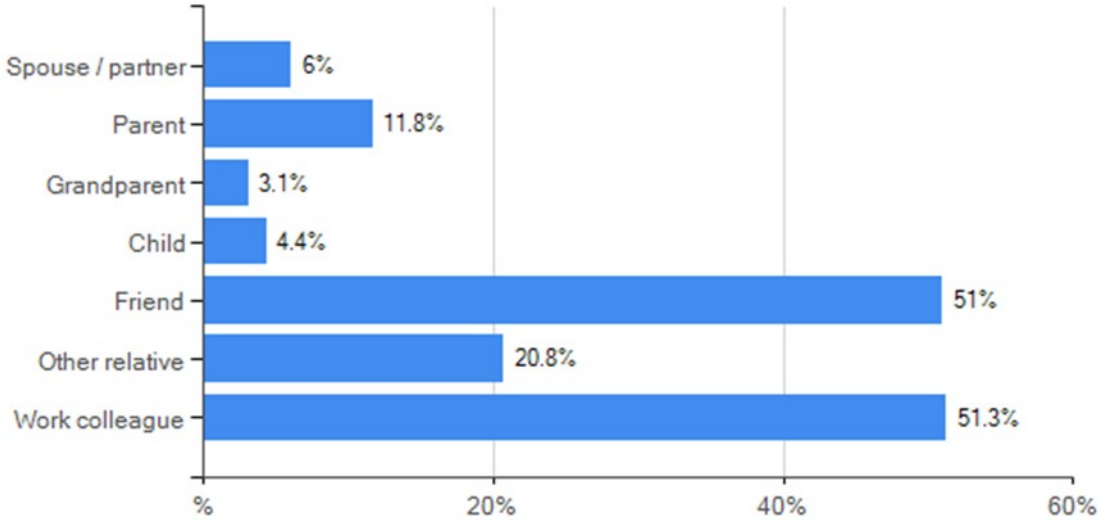
- Australian businesses
- The Australian Federal Government
- Australian state and territory governments

The threat to Australian citizens was rated as **7**, indicating that experts felt businesses and the government were dealing with more threats than the general community, but only slightly so.

More than half (**50.6 per cent**) of survey respondents experienced personal data loss by an online service provider in a cyber security data breach. Also, **11 per cent** had experienced some form of online bullying or trolling, **5.3 per cent** had experienced data theft from spyware or a hack on their device and, surprisingly, **8 per cent** of cyber security professionals had lost money due to an online scam. The rates of occurrence in the general population - who do not have an awareness of cyber security threats and the techniques used by scammers and cyber criminals - are likely to be much higher.

Based on our survey, **76.4 per cent** of cyber security professionals know at least 14 people within their family or personal network who have experienced one or more of the following:

- Ransomware - encryption of their data on their device
- Paid money due to doxing / online blackmail
- Data theft from spyware or hack on their device
- Suffered from online bullying or trolling
- Lost money due to an online scam



- ***Distribution of relationship to the impacted people with their network.***

A substantial **81.4 per cent** of respondents believed Australia is susceptible to information manipulation or psychological operations from foreign governments, with only 2.4 per cent stating this is not a threat and **16.3 per cent** unsure. On a scale of 1 to 10, with 10 being extremely capable and 1 being very low in capability, cyber security professionals believed the Australian Government's ability to deal with this type of threat would be rated as **4.3**. Considering the impact and consequences of successful information-manipulation campaigns carried out by Russia on the US, Ukraine and UK, the Australian Government should be doing more to bolster the integrity and partnership of the free press in Australia. Undermining the Australian press leaves the country more susceptible to foreign governments attacking our democracy.

When asked who in the community is most vulnerable based on age to cyber threats, cyber security professionals ranked the most vulnerable to least vulnerable age groups as follows:

Most vulnerable:	Adults 65+
	Secondary school children
	Adults 44 to 64
	Primary school children
	Young adults 18 to 24
Least vulnerable:	Adults 25 to 44

When questioned as to the cyber security threats the Government should focus on, the results were:

- 25 per cent - foreign intelligence services interference with our government
- 11 per cent - ransomware
- 10 per cent - email and phishing attacks, malware and protected DNS
- 10 per cent - critical infrastructure (all sectors and councils)
- 8 per cent - data loss mitigation
- 8 per cent - IP theft

Foreign governments have used social media sites to spread and target citizens with "fake news" or false advertising to interfere with as an example, the US 2016 presidential election outcomes, assist with the Russian annexation of Crimea from Ukraine and interfere with the United Kingdom's Brexit referendum. A weighty **81.4 per cent** of respondents believe Australia is susceptible to similar foreign government campaigns to undermine our democracy, with only 2.4 per cent confident that information-manipulation campaigns and associated forms of warfare were not an issue for Australia. For those who believed it was an issue, they rated the Australian Government's ability to be prepared and deal with the threat as low (**4 out of 10**).

2. Do you agree with our understanding of who is responsible for managing cyber risks in the economy?

Keeping Australia cyber safe and secure is a shared responsibility among:

- The three levels of government
- Business, comprising big, medium and small
- Domestic and overseas service providers
- The Australian public
- The education system - raising awareness of cyber risks and privacy impacts from K to tertiary.

The degree of responsibility varies accordingly and is not only legislatively driven but can be driven by education (awareness and behavioural change), labelling, leading by example and through various grants or tax incentives.

A major imperative is to ensure trust without an abuse of power or overreach, maintaining privacy and civil liberties while driving down complexity and costs for businesses and consumers.

3. Do you think the way these responsibilities are currently allocated is right? What changes should we consider?

There is scope for greater governmental involvement and proactivity, however, it is important that changes in responsibility do not impinge on civil liberty and privacy.

Members feel the Government could do more to share its threat intelligence and defensive capabilities, and could allocate more resources to help private enterprises deal with breaches (**prior** from intelligence gathering, **during** an incident to identify and limit damage, and **post** to assist with clean-up and remediation).

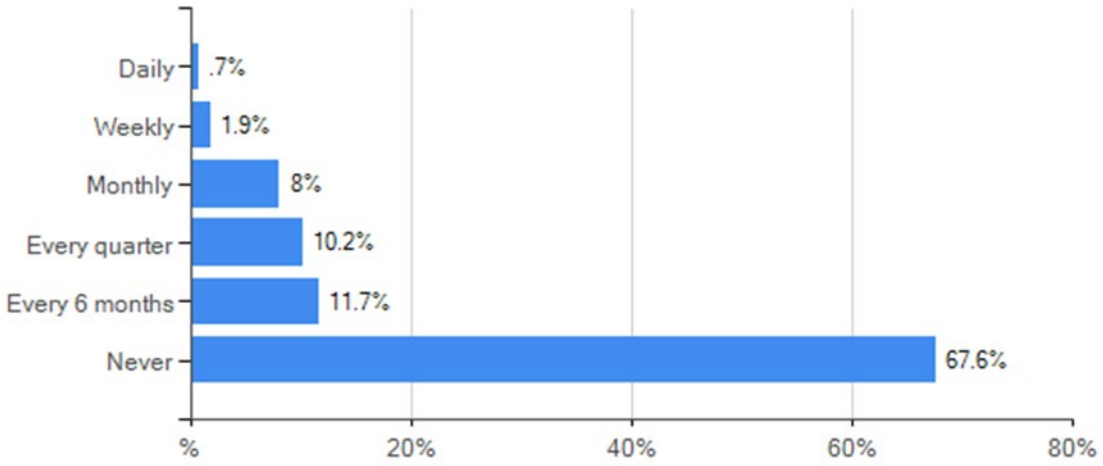
The Australia Government also needs to lead by example in its own cyber-security practices, procedures and protocols. There is an understanding that some agencies and departments are struggling to adopt the ASD Essential Eight and the perception is that if government is struggling to adopt a recommendation from ASD, there is no hope for small to medium businesses and in some cases, large enterprises to adopt the Essential Eight.

Almost **50 per cent** of cyber security professionals responded **'no'** when asked if the ASD Essential Eight should be simplified to increase adoption, only **25.5 per cent** said "yes" and the remainder

where unsure. Even with the failings of government agencies adopting and implementing the Essential Eight, an overwhelming **78.2 per cent** believed it should be legislated as mandatory for all levels of government and Australian businesses.

At the same time, the Government needs to be mindful of overreach with businesses and the community. In fact, **60.5 per cent** of AISA members believed the Federal Government had disproportionally shifted the burden of cyber defence and protection to consumers and end-users rather than building national cyber defences to protect Australians and the economy.

The Australian Government also needs to consider its own ability to deliver on what is promised. Based on the 2016 cyber security strategy and the expectations of certain deliverables, it is clear the Government has failed to execute correctly. For example, the concept of the Joint Cyber Security Centres to enhance collaboration among industry, academia, government and law enforcement was an excellent idea. The execution, however, has been poor with **67.6 per cent** of survey-takers never visiting a JCSC. The chart below demonstrates the lack of engagement between the JCSC and the security sector in regard to the frequency they are used to collaborate.



While **69.3 per cent** of respondents knew they could report cyber-security incidents and crimes through the Cyber Issue Reporting System, established by the Australian Cyber Security Centre, almost **a third** did not. This lack of awareness is expected to be much high among the community and business.

From AISA's perspective, all individuals in the cyber-security industry should know cyber incidents can be reported through the Cyber Issue Reporting System. More industry professionals were aware that scams can be reported through the ACCC (over **80 per cent**), while only **53.5 per cent** were aware they could report online abuse, including cyber bullying, image-based abuse, and offensive and illegal content to the Office of the eSafety Commissioner. What is more concerning is that only **43.8 per cent** were aware of the Australian Federal Police (AFP) portal that deals with reporting inappropriate behaviour found online towards children (for example, adults acting inappropriately with or towards a child or seeking a child for sex).

4. What role should government play in addressing the most serious threats to institutions and businesses located in Australia?

A considerable **89.3 per cent** of industry professionals believed the Government should take a more active role in protecting Australian businesses and citizens while still upholding civil liberties and privacy.

The Government should consider:

1. Improvements in pursuit and prosecution of cyber criminals and other attackers, especially those located overseas
2. Requiring minimum standards of cyber security for businesses, with incentivisation to comply
3. More hands-on help to prevent and remediate cyber attacks, especially for critical infrastructure and non-governmental essential services (e.g. education, healthcare sectors, etc)
4. Increased awareness and education for businesses and the general public

5. How can government maintain trust from the Australian community when using its cyber security capabilities?

Trust is a necessity for government, and building and retaining that trust is critical especially to digital service-delivery initiatives.

It is a balancing act for government, which must deploy its powerful capabilities to keep Australians safe and the economy secure but at the same time continue to respect the rights of the individual and those of private enterprise in our liberal democracy.

As such, any law changes and measures taken should not be for the Government's benefit at the expense of the people's.

Fear, Uncertainty and Doubt can be counterproductive and shouldn't be used as a tactic.

When governments flag a desire to act 'proactively', that should never manifest as heavy-handedness or acting without the consultation and consent expected by enterprise and individuals.

Key considerations:

- Appoint a dedicated cyber security minister. The portfolio is so important and impacts so many aspects of our economy, society and citizens that it deserves a dedicated minister. Australia has a dedicated cyber ambassador, but no dedicated minister. As we become more digitally dependent the role of this function will continue to increase in importance.
- Consult more broadly with the industry and community and take onboard the recommendations from those outside of government (industry and academia) who are better placed to understand the consequences, impacts and operational effectiveness of legislation, policy and frameworks the Government is considering.

- Establish an expert panel consisting of at least 30 industry individuals from across various sectors and ensure a good mix of CIO/CSO/CISOs from retail, banking, insurance, manufacturing, utilities/services, telecommunications, healthcare, resources and at least 10 academics from cyber security, law and humanities (ethics). Representation from vendors should be kept to a minimum as the objective of the expert panel is to advise from a whole of Australia perspective to protect businesses and the community.

6. What customer protections should apply to the security of cyber goods and services?

In our view, consumer protections should be equivalent to any other product or service.

Among the many suggestions from surveyed AISA members were:

- Anyone who is selling technology or technology services should be held responsible for 'enforcing' security standards in what they sell to business and consumers. The Government should be responsible in overseeing the security standards to which technology vendors legislate to enforce compliance.
- Imported goods must have protection installed before being used/sold to a user or consumer in Australia.
- Of value would be standard benchmarks that are easily understood by consumers.

7. What role can government and industry play in supporting the cyber security of consumers?

Regarding the cyber security of consumers, while government is making inroads through awareness and other mechanisms, our member base and Board feel that there is opportunity to state a clearer set of parameters to influence general buying decisions and behaviour. For products, digital services, online platforms etc, a system likened to the **health star rating system** used on many food products in supermarkets could offer greater simplicity.

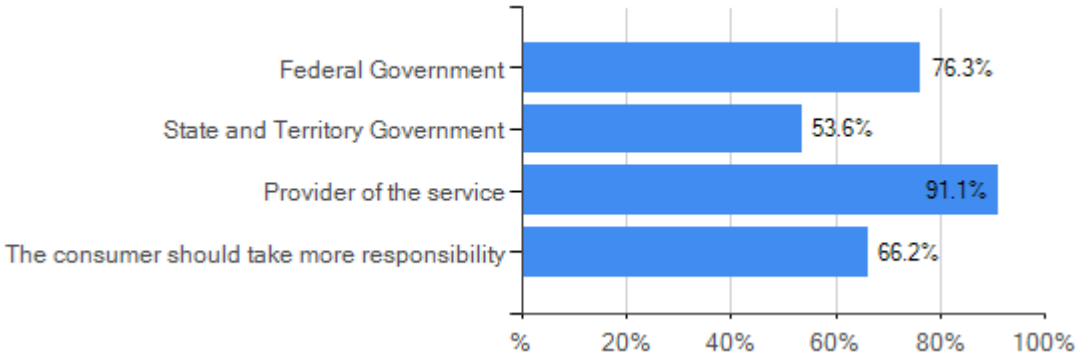
Additionally;

- Government can continue to refine and develop privacy laws to be stronger and more effective
- Government can influence the acceptable base level of security of Internet of Things (IoT) devices developed in Australia and set a minimum benchmark of those imported
- For the private and public sector that hold particularly sensitive or high volumes of consumer information, incentives could be put in place to encourage robust measures and controls to protect the information. In our survey, **78.6 per cent** of AISA members stated there should be specific market incentives to improve cyber security.
- Continue to develop **staysmartonline.gov.au** resources by:
    - Spreading the contained messaging through industry groups and newsletters

- Refine and simplify a subscription model to the content to allow consumers to be 'drip fed' engaging content over time
- Develop quizzes, and video content to allow for easy consumption

- Industry can better 'bake-in' security at the design phase of systems, applications and digital services, to ensure at the time of production, they're not vulnerable to cyber attack.
- Where good practice frameworks or guides are adhered to, industry can better brand and promote these alignments or certification to consumers (such as PCI DSS, Essential Eight, ISO/IEC 27001) to provide better purchasing decisions.

- ***Below are the results of the survey regarding who should play an increased role supporting the cyber security of consumer (respondents could select multiple answers).***



8. How can government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?

From the AISA survey, **60 per cent** of our members felt the following two mechanisms would be the most effective way to increase the security, quality and effectiveness of cyber security and digital offerings:

1. Raise awareness of and execution within the JCSCs
2. Increase awareness and collaboration through more events, at varying times, and through various channels (e.g. webinars, information packs, collaboration sites)

This is in conjunction with the responses listed under questions 6 and 7.

9. Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?

Any devolution of current government function to the private sector would need to be extremely closely considered and measured prior to any decision being reached. The obvious risk in doing this, is that commercial interests would take focus possibly over intent and independence. Not-for-profit organisations, such as AISA, somewhat negate this potential conflict and a good example of where

this can work has been the collaboration between the ACSC and AISA to host Australia's leading cyber-security conference (the Australian Cyber Conference, which was held in October in Melbourne).

With this said, as with other areas of safety and security in our society, the majority of the functions that government provides relating to policy, governance and oversight through the ASD and ACSC should and must remain with government.

Some potential functions that should be considered by government for devolution to the private sector (specifically unbiased entities and associations) may be:

- Australian Cyber Security Hacking challenge (CySCA)
- Consumer and SMB specific cyber security awareness programs (StaySmartOnline)
- Activities and events hosted within the JCSCs

10. Is the regulatory environment for cyber security appropriate? Why or why not?

Unlike other security sectors (personnel/electronic/physical security) there is no regulation of the cyber-security sector in Australia at a professional level, partly due to the diversity of the roles and job tasks (e.g. no single definition of roles as many job functions are a subset of other roles or cut across various functions in an organisation). The lack of regulation of individuals working in the cyber-security environment may place government, business and the community at risk in some work environments, but not all.

While **two thirds** of cyber security professionals in Australia support the regulation and accreditation of cyber-security professionals by an independent body to ensure a base level of qualification and standard, similar in nature to Engineers Australia, one third of professionals do not support this approach. The complexities of highly varied cyber-security job functions (e.g. cyber-security administrator, engineer, designer, investigator, manager, executive, operator, trainer, project manager, lawyer, etc) combined with the more than 100 vendor and vendor-agnostic internationally recognised accreditations/certifications also complicates the process. What should be clearly avoided is the implementation of a domestic-only accreditation/certification, like the one currently being spruiked by a professional society that does not specialise in cyber security and is simply trying to develop an additional revenue stream.

What is needed from a professional perspective is a government mandate that cyber-security professionals need to have either a University/TAFE qualification in cyber security or an existing globally recognised industry based accreditation/certification that matches the job or role function. Examples of globally recognised organisations producing vendor-agnostic accreditations/certifications include ISACA, ISC2 and CompTIA. A mapping of vendor and non-vendor accreditations needs to be developed and adopted to role functions like the USA DoD Directive 8140/8570.01-M to help normalise the more than 100 existing accreditations to job functions and roles.

Further information about USA DoD Directive 8140/8570.01-M can be found at:
https://partners.comptia.org/docs/default-source/resources/certification_dod_8570_flier.pdf

While the above link highlights CompTIA certifications, it also highlights other certifications from other vendor agnostic providers against DoD job functions. A similar mapping free from commercial interference needs to be developed for Australia.

The Government could further implement a clearance process with two tiers (basic and intermediate) that, combined with a solid educational grounding and vendor-agnostic certification, would place individuals with all three as trusted and vetted individuals. This would also enhance the pipeline for cleared individuals to work in industry and with government.

Of those surveyed, **58.1 per cent** did not regard the current regulatory environment for cyber security in Australia as appropriate. Only **5.3 per cent** believed it was appropriate while **36.5 per cent** were unsure.

It should be noted that over **62 per cent** did not support the Australian Government signing the CLOUD Act with only **6.7 per cent** in support.

In regard to the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA), only **9.2 per cent** believed it should **not** be amended while an overwhelming **62 per cent** believed the current legislation had flaws and needed to be amended.

11. What specific market incentives or regulatory changes should government consider?

Our survey showed that **66 per cent** of industry professionals believed the Federal Government should pass legislation to ensure cyber security is deemed a business priority. The example used was extending APRA's CPS 234 requirements to all businesses and not just financial institutions.

Almost **72 per cent** of AISA members favoured the Government legislating the cyber security equivalent of seatbelts in vehicles, to raise the bar of cyber-security maturity and compliance.

Suggested measures from our survey include:

- All ASX listed business to report on cyber-security readiness as part of a legal requirement similar to prudential requirements
- An independent government body, similar to the ATO, to conduct audits on businesses. Not just for compliance, but to make sure that the right controls are in place
- Continue to support Australian cyber start-ups, particularly those offering services to SMEs and offer subsidies for SMEs to make use of those services
- Define a minimum level of cyber capability (e.g. USA DoD Directive 8140/8570.01-M)
- Provide business tax incentives for expenditure on cyber-security personnel and training (not on products).
- Certification system that requires all businesses who trade to have a cyber accreditation of some level. The UK 'Cyber Essentials' https://www.cyberessentials.ncsc.gov.uk/ could be used as a starting point.

Other measures include:

- Tax breaks to meet the Essential Eight, definitions and road maps
- Accreditation akin to a cyber security star rating system for some consumer products.
- Widen access to the small business cyber security grant to boost small-to-medium businesses
- Mandate that company directors should receive a minimal cyber security training

12. What needs to be done so that cyber security is 'built in' to digital goods and services?

Of respondents, **80 per cent** believed that listing security features on products and services would drive better consumer choices.

And **81 per cent** thought that manufacturers and suppliers of IoT devices and services should be responsible for security for the life of the device/service.

Meanwhile, **69.2 per cent** agreed that customer protections should apply to the security of cyber goods and services, with **2.5 per cent** disagreeing and **28.3 per cent** unsure.

The survey expressed a view that the only way to drive security in IoT, especially those devices that have the ability to impact the health and well-being of citizens (medical devices, cars, etc) would be to regulate it to require manufacturers to meet certain standards.

IoT devices need to be more tightly regulated to require they meet minimum standards, are able to be updated and are updated, are supported for some minimum lifetime and responsive to bug reports by pushing out updates. The US state of California is leading the way with this type of legislation and, while not perfect, is a start in the right direction. For further information please see SB-327 Information privacy: connected devices (https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327).

The average citizen should not be expected to be an expert in cyber security, so manufacturers should have more accountability.

A star-rating system for the level of security on a product, certified by the Government could be useful for consumers. However, the rating system needs to be backed by advertising and marketing and must convey to the consumer a value.

13. How could we approach instilling better trust in ICT supply chains?

All supply chains should be resilient and verification should be based on standards. It must be a collaborative effort between private and public parties. No single vendor, operator or government can do it alone.

There needs to be greater transparency when it comes to the Government monitoring the ICT industry either through the Access Bill or otherwise. Respondents have indicated that they cannot expect foreign companies to have trust in their services when they do not know the activities of our own Government.

14. How can Australian governments and private entities build a market of high quality cyber security professionals in Australia?

Of respondents, **83.5 per cent** agreed there was a cyber-security shortage in Australia with the majority agreeing it was the level of quality and diversity of skills that was deficient. Respondents agreed that there were few very highly qualified professionals but those at the start of their career in cyber security cannot secure roles due to unrealistic experience expectations of the Australian Government and private sector. AISA's recommendations are for government to provide some type of incentives for businesses to employ new graduates and for education providers to provide more realistic hands-on experience dealing with cyber security holistically (for example, cyber defence, consulting, architecture, governance, operations, risk management, policy and regulations, etc). The current skills-gap challenge also demonstrates the body currently accrediting cyber-security courses in Australia is not working with industry to ensure courses are aligned with the needs and expectations of the business community. To further compound the issue, the organisation in question also has a conflict-of-interest to resolve (that is, charging for membership and accrediting courses) AISA supports moving this function back to government or a body specifically focused on delivering course accreditation without charging or indirect financial benefit to remove the conflict of interest.

The shortage of appropriately skilled individuals is also being created by a combination of factors including:

- The Australian education system – not enough properly trained teachers and in some cases poorly designed courses that do not reflect the current needs of industry
- Lack of government strategy,
- Lack of parental appreciation of the career opportunities available which results in reduced or little encouragement to pursue a career in technology, engineering, maths computing skills or qualifications required to work in cyber security
- An unwillingness by business to employ graduates, viewed by business as lacking people skills and hands-on experience. Consequently, business views graduates as taking longer to become productive within the context of their business as opposed to poaching an experienced candidate from another organisation.

Companies are encouraged to increase their capabilities and be more willing to train staff members. Some respondents suggested an industry-recognised cyber-security-skills framework would be of assistance.

While most education providers have or are in the process of building Security Operation Centres (SOC) to act as simulated training centres, Deakin University has gone two steps further by building an operational SOC to provide real world hands-on experience and, in addition, included missing pillars of educational experience in cyber-security consulting (design, architecture, audit and governance) and operations (device management, patch management, data backups, etc). While this model should be commended, a government-coordinated approach to building the three pillars across the country is needed to lift the entire sector from an education experience for students (as not all students will want to become SOC analysts), but also from a skills capability of the educators who often lack practical hands-on business experience which is needed to help shape the next generation of the

workforce.

While most Universities and TAFEs have Work Integrated Learning (WIL) programs that place students in a paid internship placement in industry for 3-12 months, the uptake from industry is slow as the students often lack the well-rounded experience and soft skills to integrate seamlessly into organisations that are already capacity constrained and lack the time to handhold new recruits. Incentives such as tax breaks or grants to take on Australian domestic students may increase the adoption of internships by major Australian organisations.

In some instances, particularly for large organisations, there should be probity checking of cyber-security professionals performing work in Australia or the development of improved processes with existing security-clearances processes (basic, NV1, etc) to enable organisations to put their staff through the clearance process at the cost of the organisation or individual. This would dramatically increase the pool of vetted resources in Australia and shorten the delivery time on projects that require vetted staff. Currently, vetting is performed when an individual is tied to a project, however by opening up the application process dramatically increases the number of industry ready people with clearances.

Recognition by government of the need for ongoing training and professional development through tax breaks/incentives or other funding models should be considered. This would also help address the skills shortage in this area. A partnership between key stakeholders (including government and private industry) should determine the skill levels required to build cyber-security capability and integrity.

15. Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?

Value is seen as the biggest impediment to cyber insurance. Often people will only obtain insurance once they have been exposed to a cyber threat. Standardising insurance definitions may assist so that consumers know what the insurance covers and what it does not cover. For instance, some insurers will not pay on a claim where the attack could have been committed offline. In other instances, insurers will only pay based on actual money loss, not on loss of reputation or for pursuit or defence legal fees.

Reduced premiums based on adequate training and proactive cyber resilience frameworks should be mandatory.

16. How can high-volume, low-sophistication malicious activity targeting Australia be reduced?

Advice from our surveyed members strongly encouraged a push for greater awareness and education, including a widespread and sustained awareness campaign to drive behavioural change.

Other suggestions included:

- Blacklisting the culprits/source addresses at the ISP level

- Business incentives to deploy the Essential Eight (Strategies to Mitigate Cyber Security Incidents) such as tax breaks
- Making sure all business have DMARC (Domain-based Message Authentication, Reporting and Conformance) setup for email with SPF (Sender Policy Framework) and DKIM (Domain Keys Identified Mail)
- Taking proactive steps to alert the millions of users with insecure routers and modems in their home to their risk and how to mitigate it
- ISPs playing a direct role in detecting potentially malicious outbound connections and having in place processes to flag or notify their users and provide mitigating controls
- Detect and eradicate spam voice telephony campaigns that target all but often affect the most vulnerable members of society and have far-reaching consequences

17. What changes can government make to create a hostile environment for malicious cyber actors?

While only **5 per cent** of respondents felt it was not possible to create a hostile environment or that a hostile environment would have adverse impacts to business and achieve nothing, **95 per cent** of respondents felt there were several activities that could be undertaken by the Government to help reduce the occurrence of malicious activity and deter cyber actors from attacking Australians.

Of respondents, **26.4 per cent** felt that greater penalties for cyber criminals would be a deterrent, particularly for threats coming from the local environment or partner countries. Diplomatic responses using global cooperation, international law or various sanctions to create economic hurdles were considered an alternative approach for foreign threats by **12.9 per cent** of respondents. Awareness and education was also recommended by **13.5 per cent**, including education on the responsibilities of data custodians and owners, while **17.2 per cent** considered that the Government take a more hands-on approach with offensive active responses, effectively hacking back. Deploying deception or disruptive technology (honeypots) across the Australian environment, including some small business environments was suggested by only **3.7 per cent** of respondents, so too was the suggestion to name and shame state actors, deployment of clean-pipe technologies (content filtering, SPF, DKIM, DMARC etc) and to work in greater collaboration with industry were all considered by **4.3 per cent** of respondents as actions to take.

Additional suggestions included more resources for the AFP and ACSC, improved software from vendors, mandatory assessment of systems (similar to civil engineering), additional resources specifically for small business and to support victims.

Key findings
26.4 per cent - greater penalties for cyber criminals.
17.2 per cent - boost offensive response.
13.5 per cent - improve community and business awareness and education.
12.9 per cent - improve diplomatic response and standing (normalisation of international laws).

18. How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?

Key areas that were identified to help remediate cyber risks are:

1. **17.9 per cent** recommended improved education, training and awareness was required to highlight the risks, increase non-technical cyber-security discussions at the board level relating to organisational risk and cyber resilience. The concept of building security champions within organisations (e.g. developing cyber ambassadors) should be further explored
2. Greater intelligence sharing between government and industry with government taking a more active role in identifying weaknesses in the Australian environment and contacting those organisations to ensure they proactively remediate through patching, hardening, segmentation was recommended by **13.1 per cent**
3. Ensuring organisations understood the ASD Essential Eight, got the basics right but also made recommendations that outlined how to apply the Essential Eight either through technology (open source and/or proprietary), process changes or behavioural change was recommended by **11.9 per cent**. Asking people to be compliant with the Essential Eight isn't enough as the pathway to become compliant needs to be low cost, not time consuming and easy to follow (step-by-step recommendations or checkbox toolkits for business to follow would assist adoption)
4. Guidance and training on improved risk-management practices
5. Allocation of more resources by the Government (funding and people) to help lift capability and maturity
6. Improved lower-cost tools for detection, remediation and automation
7. Some in the sector also supported the adoption of a compliance statement as a tick box when logging tax returns in relation to ASD Essential Eight adoption to drive behavioural change
8. Australia should look to the US, in terms of practice guidance and implementation guides rather than just enforcing standards
9. Creation of a reporting system (like DNSRBL) which scores reputation of an organisation based on reported/notified security issues (like those reported to ACMA). Hence, the establishment of Digital Trust Agency. Data could be publicly available to other organisations as a way to lift the standard of security maturity and capability in the supply chain (an alternative approach to CPS 234, which lets market forces drive change). Hence, consumers would want to only shop or work with organisations with a "high trust mark".

19. What private networks should be considered critical systems that need stronger cyber defences?

- Services that aggregate personal data

- Providers/services that are used by a majority of major organisations in a sector (eg, the major banks using Amazon Web Services). Any catastrophic instance in Amazon would negatively impact the financial system, particularly at times of war
- Services/organisations that are used for safety management
- Any cyber-physical system that does or may cause pollution or contamination of the environment if improperly operated
- All systems associated with emergency services, logistics, finance, health, public utilities or used in the production, distribution or management of water, energy, transport and shelter
- Universities and sectors focused on research and intellectual property
- ISP/telecommunications, hospitals, public transport and key services that are critical to the movement of goods, services or people that, if impacted, would harm the economy. For example, ports (shipping and aircraft).

20. What funding models should government explore for any additional protections provided to the community?

The Government could consider tax rebates or other tax incentives. Previous programs such as the Cyber Security Small Business Program, which was limited to CREST, could be opened up to allow universities to help small-to-medium businesses and authorised Managed Service Providers such as Telstra, Optus, NTT and CyberCX, etc.

It is important to remember that cyber security in an organisational challenge is not just technical but is also policy, procedure and behaviour (culture) related.

Suggested funding models:

1. Grants
    a. Research (focused on uplifting community protection, behaviour change, etc)
    b. Uplift of capability and maturity of small business - which are undertaken by professional organisations like large consulting, MSP, universities/TAFEs and banking (using students) to lift their business customers
    c. Subsidise training
    d. New cyber-security initiatives

2. Tax incentives (rebates, levies, reduction in payment, deductibility, etc)
    a. To drive adoption of Essential Eight
    b. To employ Australian graduates (citizens) who have recently completed cyber-security undergraduate or postgraduate (e.g. first employment opportunity) at accredited Australian universities and TAFE. Incentive is only given if the graduate stays for more than 12 months
    c. Ability to write off cyber-security solutions/cost of reviews to drive adoption and lower the overall cost to businesses

3. Scholarships
    a. To boost women, indigenous and rural students in cyber security. The current industry diversity is **13 per cent** female and **87 per cent** male
    b. To help retrain people from other disciplines (returned veterans, workers from sectors in decline, etc).
4. Research
    a. Another mechanism to improve collaboration among government, industry and academia at the JCSC level in each state is to allocate a funding pool that will match contributions from industry (Australian businesses). Each JCSC can establish an advisory panel that would work with industry partners and university researchers to coordinate valuable multidisciplinary projects that benefit Australia. Projects could be short term (less than one year leveraging postdocs), extend to three years (relying on PhD students) or a combination of short-term objectives and a three-to-four year horizon. This program would be open to a wider range of partner businesses in industry, academics from all universities and would be overseen by each JCSC. Similar in operation to the Oceania Cyber Security Centre (OCSC) based in Victoria, but replicated across the nation. OCSC could move into the JCSC and facilitate research in Victoria, as an example. This model would drive engagement, be inclusive (any university can participate), drive multidisciplinary approach, removes duplication and would be transparent and open. ACSC could manage and coordinate single source of truth, listing the research projects with their status (proposed, inflight, completed, declined) and their expected completion date and impact to society. This would also give the Government early line of sight of technology or projects that may be useful to be adopted or further explored in the national interest. Funding for projects can be 50 per cent by industry and 50 per cent by government

21. What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?

Members indicated there was considerable room for improvement concerning the Joint Cyber Security Centres, with **67.6 per cent** saying they had never attended a JCSC and only **1.9 per cent** reported that they used a centre weekly.

Suggestions to consider:

- Security clearance procedures could be improved to create a pool of cleared individuals, ready to work
- Enable any cyber-security professional to apply and pay their own way to undergo a basic or NV1 security clearance assessment

- Define and establish clearer guidelines for reporting vulnerabilities between commercial organisations and government.
- Ensure the JCSCs have people who have a wide range of skills to support the needs of the community
- Establish funded research clusters at the JCSCs across the country to improve collaboration in each region. Ensure this is open to all universities and Australian organisations.

22. To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?

If consumers do not, through their buying decisions, demand digital products and services that are safer then it is less likely that the makers will market more secure offerings (in the absence of government regulation). Awareness would help drive this demand.

Purchases, especially the more expensive ones are complex and emotions can often play a factor. Therefore, awareness could expand to include the notion of keeping loved ones protected with safer goods and services.

A rating system such as energy stars could work to influence decisions. But we see consumers choosing less efficient air-conditioners and fridges, for example, because they are cheaper upfront. The more efficient appliances are cheaper over the longer-term, however, due to lower power costs. And so a rating system for cyber would need to make clear the cost-benefit of additional stars.

23. How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?

In conjunction with awareness campaigns and regulation, consumers will demand cyber secure products. There is international and domestic government support for cyber-secure products, however, investment from Australian businesses into cyber-secure products is substantial and may not be viable, without government incentives.

Of respondents, **65 per cent** believed the Federal Government should pass legislation to ensure cyber security is 'built in' to digital goods and services to provide a minimum level of safety.

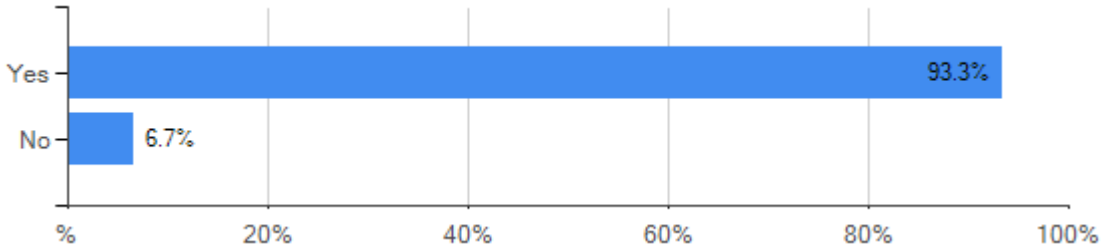
24. What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?

Behavioural campaigns should be targeted to different segments of the community; the messaging to youth should be distinct to that of an older age group. Elders in the community need more digital awareness on attacks such as phishing and scams while the younger generation needs to be trained to be safe on social media and online gaming.

With a more widespread consumer campaign, positive messaging rather than a scare campaign will empower individuals. The message needs to be widespread to penetrate the marketplace and ensure the message is heard about the importance of cyber security. Testimonials from real-life experiences

make the campaign relatable; 'it could happen to you/someone in your family' to enact behavioural change.

When asked "Do you believe the Australian Government should develop and launch a comprehensive behavioural change campaign similar to the "Slip, Slop, Slap" anti-cancer campaign, as an equivalent for cyber security, to raise awareness across all segments of society and drive behavioural change" an overwhelming **93.3 per cent** of security professionals agreed (graphic below).



Examples of other programs include:

- Quit campaign – health promotion campaign
- Dumb ways to die – safety around Melbourne trains campaign
- Heart tick of approval – health promotion campaign
- Speed kills – safety campaign
- The Grim Reaper – AIDS awareness and safe sex safety campaign
- Buy Australian – reduce imports and keep jobs in Australia campaign

Lessons can be learned from the health-promotion sector as the campaigns in this sector are often linked to a benefit - the 'what's in it for me' aspect - and are designed to be remembered and drive behavioural change.

25. Would you like to see cyber security features prioritised in products and services?

Almost **80 per cent** of respondents believed listing security features on products and services would drive better consumer choices. Whilst it may not change behaviour initially, we would recommend linking it into awareness campaigns around cyber security, which would raise overall awareness. Respondents suggested a star rating or tick of approval for the level of security of the product, certified by government.

Of respondents, **76 per cent** believed there should be market incentives to improve cyber security including tax incentives, grants, providing free cyber short-course training to SMEs to ensure that cyber-security features are included and to increase awareness levels.

26. Is there anything else that government should consider in developing Australia's 2020 Cyber Security Strategy?

- Bipartisan approach to the cyber-security strategy to cross over change of governments
- A cyber-security strategy that has measurable outcomes that can be tracked
- A focus on building capacity and sustainable resources
- There needs to be improved coordination among all three levels of government (federal, state and local) to remove duplication and competitive programs so Australians get the best value for the level of expenditure
- A focus on collaboration between governments, academia, businesses and peak bodies

And **71.4 per cent** of cyber security professionals believed the Australian Government should independently certify and accredit cyber security undergraduate, postgraduate, TAFE and tertiary programs to ensure they met the needs of Australia and industry.

Contributors to this response includes:
AISA members and partner organisations across Australia
AISA board and staff

Australian Information Security Association
ABN: 181 719 35 959
Level 8/ 65 York Street, SYDNEY, NSW, 2000
Phone: 02 8076 6012 Email: admin@aisa.org.au Web: www.aisa.org.au