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

7 November 2019

Dear Minister

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

Deakin 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 provides cyber resilience for all Australians.

While the original strategy from 2016 was a great start to improve national cyber partnerships, building stronger cyber defences, establish global responsibilities and influence, drive growth and innovation and build a cyber-smart nation, the effectiveness of the execution has been limited and the diversity and inclusiveness of wider sectors was constrained. The threat environment to Australia's economy has exponentially increased with 1 in 3 Australians now impacted by cybercrime.

Since 2003, Deakin University has been a leader in cyber security research, education and innovation in Australia. Deakin has been awarded cyber security educator of the year for three consecutive years and has a range of undergraduate and postgraduate courses focused on cyber security, including combined undergraduate degrees with law and criminology. In 2020 Deakin is bringing to market an Australian first Industry Cyber Security PhD program designed to build the PhD pipeline at an executive level, but also develop highly critical business focused applied research. Deakin jointly with NTT (formally Dimension Data) supports Australia's only dedicated cyber security start-up accelerator, CyRise, now in its third year.

Deakin takes a holistic approach to cyber security, which includes Artificial Intelligence (AI), Information Technology (IT), data analytics, engineering, business and law, psychology, humanities and health as these fields directly intersect with the future of our economy. This response is guided by the Deakin values of being excellent, ethical, inclusive and sustainable.

Yours sincerely

[redacted]

Damien Manuel
Director of Cyber Security Research and Innovation

Centre for Cyber Security Research and Innovation
Deakin University
Email: [redacted]
Tel: [redacted]

Burwood Campus,
222 Burwood Highway, Burwood, VIC 3125
deakin.edu.au

Deakin University's specific response to the call for views

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

Deakin observes four target vectors in the cyber threat environment:

1. **Technical:** Software and networking, inclusive of Adversarial Artificial Intelligence (AI), IoT (Internet of Things), malicious software and dark web.
2. **Physical:** Hardware, specifically altered and compromised devices, inclusive of hardware attacks, as well as propagation of attacks across the connected network of hardware devices.
3. **Personal:** Impacts to individuals of activities such as phishing, extortion, brand jacking, cyber bullying, online grooming, cyber-enabled gaslighting, spyware and breaches of personal privacy.
4. **Societal:** Fake news, dilution of trust in institutions and information manipulation.

These target vectors are relevant beyond economic entities to pose threats to critical infrastructure in utilities, power distribution networks, medical services, (formal) education, and erosion of trust through manipulated public perception of products and services.

We posit multi-pronged approaches to address these threats, comprised of technical capability, social awareness and education, and physical security, in different measures, appropriate to the context.

Manifestation of these addressment strategies requires holistic understanding of the shared responsibility involved from businesses, consumers and the government to effectively engage with and enact these security provisions. It is also important to consider the motivation of the various threat actors (organised crime, nation states and hacktivists) as foreign policy, domestic policy, ideologies and corporate decisions will all impact their activities.

Much greater emphasis needs to be given to the general area of cyber crime. While the government has been particularly vocal around state actors targeting national security, the reality is that cyber crime related incidents are vastly greater in number and increasingly damaging businesses and the economy. This threat is only going to increase.

Prior to 2014 the government had a dedicated unit based in the Australian Government Information Management Office (AGIMO) established to support non-national security agencies in the federal government in terms of cyber security related matters. This unit was focused on new ICT capability being developed for agencies and provided guidance to Cabinet and those agencies as part of the normal consideration of 2-Pass business cases and New Policy Proposals (NPPs). This capability was abandoned in late 2014 and subsequent efforts to re-establish it diverted to other areas. It is no coincidence that during the period 2015 to 2019 we have witnessed a far greater incidence of non-national security agencies being compromised or demonstrably failing to improve their cyber assurance performance. Government needs to re-establish this function and it must be placed outside the national security functional area.

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

To adequately protect Australia, the following play a part in managing cyber risks to the economy:

- government and associated federal, state, and local council agencies
- large enterprise and small to medium businesses, including the various supply chains
- providers of services, both onshore and offshore
- Australian citizens (consumers)
- schools: providers of basic awareness of cyber risks and privacy through their curricula.

The degree of responsibility varies accordingly and is not only legislative driven, but can be driven by education (awareness and behavioural change), labelling, leading by example and through various grants or tax incentives. Broader and definitive public / private collaboration is necessary to address the challenges. Please refer to question 6 for additional information where government can be the lead and other instances where industry needs to lead, but should be funded or assisted by government.

Consumer protection laws are an area that needs focus and harmonisation across the federation. A key legislative element will be the recognition of data as property in the criminal codes. Calibration and coordination is required to ensure unauthorised data destruction can be prosecuted criminally and pursued through civil actions.

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 both businesses and consumers.

Government agencies are presently investigating or implementing numerous overlapping technologies, including cloud solutions to transfer operations or management to a third party. Many of the lessons learned remain with the implementing agency and much of the power that could otherwise be achieved through a consolidated effort is lost due to lack of trust between departments, or lack of central oversight. The Australian Cyber Security Centre (ACSC) is well placed to provide guidance to agencies adopting cloud technologies to ensure a consistent, secure approach is undertaken, whilst still maintaining flexibility many departments believe makes them unique; however, limitations with funding and availability mean the ACSC is unable to take a lead on these initiatives, which is resulting in a fragmented, high cost approach. Several private sector companies have experience advising and deploying solutions across multiple departments. It would be valuable for organisations such as ACSC to centralise the lessons learned through a community of practice or consortium so as to reduce the cost of implementation to the agencies, increase security across implementations, and provide a united model to negotiate with technology vendors.

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

Cyber risk management in an economy is a multi-faceted problem. Deakin University recommends to implement a knowledge dissemination campaign that helps the Australian population better understand the stakeholder responsibilities when it comes to cyber risk management, and to better gauge the impact of a cyber attack. It is also important to quantify the impact of not having safeguards in place against imminent cyber threats.

It is vital to have a process in place for the development and propagation of a shared responsibility model that represents all actors within the system and to scope the responsibilities that different actors within the national sphere need to be aware of, as well as knowledge dissemination around the implications of eschewing such responsibility.

Proper governance for cyber risk management can be realised through clearly articulated policies that have been drafted by the government for threat identification, management, mitigation techniques and security controls, that can be adopted for cyber risk management by all stakeholders; government, enterprises and consumers, alike.

Changes to consider include:

- Government agencies must have clearly defined road maps for risk management, leading by example and not exempt from policies applied to commercial organisations.
- Government advisories on cyber risk management must be defined and disseminated for specific application domains and/or industries; health facilities, utilities, critical infrastructure, defence, Government agencies and small/medium/large enterprises.

- Government to involve diverse range of stakeholders in the development of a risk management strategy.

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

Government has a key role in connecting Australia to worldwide issues, awareness and practices. In the same way that no single Australian company can go alone in defending itself from cyber threat, the same is true at the national level. We need to rely on international government connections and collaboration to bring home local awareness of threats, approaches to protection and response to ensure that Australia is defended from the most serious threats in a coordinated manner.

Government should focus on improving local Australian engagement through shared insight and collaboration with institutions and business. This would require a cultural change within agencies like ACSC to become more business focused, less hindered by bureaucracy and better funded and resourced to deal with the increased workload. There are currently a number of agencies performing disparate functions. Some business acumen and a clear mission would be a positive step for the sector.

A recent survey conducted, by the Australian Information Security Association (AISA) highlights that 68.2 per cent of cyber security industry professionals have never visited a Joint Cyber Security Centre (JCSC), with a further 11.6 per cent visiting only every six months and 9.2 per cent visiting every quarter to collaborate and exchange intelligence with government, academia and other commercial organisations. This represents a missed opportunity for government and highlights the lack of business acumen in the execution of the JCSC to drive engagement and collaboration. This could be rectified with improved outreach, more realistic operating hours, standardised operations, planning events with at least three month lead times and a stronger business/research focus.

Another mechanism to improve collaboration between government, industry and academia at the JCSC level in each state, is to allocate a funding pool which will match contributions from Australian industry. 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 leveraging postdocs or extended to three years by relying on PhD students or a combination of both. 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.

This operation would be similar to the Oceania Cyber Security Centre (OCSC) based in Victoria, but replicated across the nation. This model would drive engagement, be inclusive, any university can participate, drive multidisciplinary approach, remove duplication and would be transparent and open. ACSC could manage and coordinate a single source of truth, listing the research projects with their status and their expected completion date and impact to society. This would also give the government early line of sight of technology or projects which may be useful to be adopted or further explored in the national interest.

Legislative changes through grants, tax incentives or sector specific standards could act as a way to drive process improvements and uplift cyber security capability and resilience (e.g. CPS 234 is driving a wider uplift across the suppliers to the Financial Services sector). Exemptions and military export control laws which currently hinder some academic research, particularly into encryption, should be reviewed to streamline the process and unlock the research potential that exists within Australia.

As directed by board and customer expectations and legislation such as APRA's CPS 234, more companies are closely scrutinising their supply chain and outsourced service layers. This scrutiny requires significant effort to evaluate suppliers and for suppliers to respond to disparate evaluations undertaken by different customers. Government could establish standard reporting on security posture that can be trusted by the community in a manner that would both improve security and simplify reporting.

Government should examine how to incentivise industry to achieve standards of good practice that ultimately protect Australians. The 'essential eight' strategies set an expectation level that is difficult to achieve, but ultimately organisations that invest in implementing this advice are not rewarded with trust recognition. Government should examine how to convert that effort into business value at both a local and international level.

Government can play a more proactive role collaborating and sharing insights with business, while also actively disrupting cyber threat actors, working with international allies (USA, UK, Canada, NZ and others) to also improve prosecution and/or extraditions of identified criminals.

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

'Trust' is defined as the confidence one has in future behaviour, based on past performance. The government has lost the trust of the Australian community in terms of its performance in ICT. Repeated surveys undertaken during the course of this decade have demonstrated a marked decline - coming down from the high 80s in the 2011 'Use and Satisfaction of Online Services' survey to more recent DTO and AIIA surveys with trust falling to well below 50 per cent. The passing of the TOLA legislation in late 2018 has seen a significant loss of trust for the Australian ICT industry generally, and 'myth-busting' papers from ASD do not rectify this situation. The question uses the phrase 'maintain trust' which, in this context, seems to overstate the reality. The focus for government now must be how it gains the trust of Australians and industry.

It is Deakin's position that trust cannot be accelerated, but must be carefully cultivated amongst stakeholders. Deakin offers the following suggestions as how this trust cultivation can manifest:

- Minister dedicated to cyber security rather than a shared portfolio. It also signals to the market the importance of cyber security and enables a minister to focus on key priorities that are critical and cut across other ministerial portfolios.
- Key Performance Indicators (KPIs) that ensure accountability and transparency for public items, hence ensuring progress is measurable and the funding allocated can be measured against the value delivered.
- Campaigns for safety, awareness, behavioural change.
- Establish transparency with the Australian public by demonstrating that the government is actively engaging with the security community to work through challenges to adopt broadly supported approaches to national security.
- Reports on significant cyber security events, statistics on attacks and issues solved (e.g. public transport and KPIs that are met for performance) that can easily be consumed by citizens and businesses. Historical trends and data can highlight an increase or decrease in control effectiveness and changes in the threat landscape. The data could be used by businesses to determine future trends allowing them to adjust risk profiles and mitigation strategies accordingly. Data could also highlight vulnerable sectors or sectors lagging behind that may need additional funding support, better targeted awareness campaigns or legislation/standards to drive improvements.
- Broader research investment into key areas relating to defensive, offensive and areas to improve society and education (e.g. AI, IoT, control systems, energy, finance, automation, smart cities and defence). Currently research investment in cyber security is too narrow and does not include the entire capacity of the research sector. Easier access to research funds cross-disciplines, and a larger investment pool for funding that supports certain economic or commercial challenges like Homomorphic Encryption for banks is required.
- Provide greater clarity around the role of the ACSC. Currently the ACSC occupies a varied role as a policy vehicle, a coordination role, an incident responder and a quasi-commercial entity. The policy and coordination role is largely ignored and unfunded (e.g. the IRAP program) and the technical elements of the enterprise are open to conflict of interest issues due to the large contract labour force, who are actively building businesses in competition with commercial entities through the opaque operational model of the ACSC. The Australian CERT role also needs to be clarified in national incident response.

- Increasing the funding available for the Australian National Audit Office (ANAO), specifically with regards to additional cyber audit funding. Results of these audits should be published and agencies that have achieved compliance with the Essential Eight provided with ongoing funding to support the achievement. Combined with a 5 per cent reduction in agency funding (cumulatively applied) for underperformance in annual cyber security performance, independently verified by the ANAO and not the ACSC.
- Research shows the public has some concerns with the government's use of drones for various purposes, as well as information integrity and privacy. To address these concerns, the government should initiate an open dialogue with the public about these issues, to put in place mechanisms to ensure transparency concerning its use of drones and data collection, and inform the public effectively about means and methods developed to maintain and protect the data. Deakin scholars are already investigating the effects of various mechanisms and processes on public trust in government agencies.

These approaches can be designed, developed, and employed in concert with Deakin's suggestions around cyber safety and generational campaigns expanded on in the cyber aware community section of this document.

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

Consumer protections should be the same as any other product, but where digital products (including 'as-a-service' products) that connect to the internet are concerned, new expectations need to be set. Baseline security requirements should be defined and be expected to be met by vendors (e.g. admin and maintenance account password schemes). As vulnerabilities over the life of a digitally connected device can have an adverse effect on both the consumer and the community generally, there should also be guidelines set for ongoing maintenance and patching. A scheme to 'dead head' vulnerable and unsupported products and services may be required to protect the Australian community (analogous to taking unsafe cars off the road).

The government also needs to strengthen the notifiable data breach scheme to expand the number of goods and services covered (e.g. reduce exemptions of who is not required to notify) and the data behind those breaches should be researched to build case study guides for use in education and training and by industry to understand the reasons breaches occur with a view to mitigate the impact or reduce the rate of occurrence. Between the 1 April 2018 and 31 March 2019, 964 breach notifications were made, which represents a 712 per cent increase in the previous 12 months prior to the scheme, demonstrating that changes to legislation are required to drive market improvements.

However, it should also be stated that legislation alone is not helpful. Without the learnings from the scheme and without those who have been breached coming forward publically to talk openly about the challenges, lessons will not be learned that can dramatically help other sectors. The latest report from the Office of the Australian Information Commissioner (OAIC) shows that Australia is on track to report the same level of breaches as last year with very similar percentages for the cause (34 per cent human error, 62 per cent malicious or criminal attack and 4 per cent due to system faults).

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

A similar approach to the Australasian New Car Assessment Program (ANCAP) could also be applied to the security of cyber goods and services. A similar approach may drive consumers to make a better choice while pushing the market to improve security of cyber goods and services. Other similar campaigns or approaches include the Heart Foundation's tick program designed to influence consumer behaviours, the Australian Made campaign to encourage domestic consumption of Australian made items, the slip slop slap anti skin cancer campaign which encouraged sun screen use and the energy star rating system which drives improvements in efficiencies for domestic appliances such as air conditioners or washing machines. However, the success of these campaigns is dependent on a significant long running and multi-faceted marketing and education campaigns that would require ongoing commitment.

Additional recommendations:

- Government can establish minimum security benchmark for IoT devices imported into the country.
- Government can establish stronger consumer privacy legislation, akin to that in California, USA.
- Government to offer cyber security training and education programs on how to use technology for various segments of the market (e.g. young, elderly etc).
- Government to review and update domain specific cyber security guidelines for sectors like energy, water, health and finance.
- Government to provide advice on secure technologies (e.g. assurance measures such as approved security ticks / security marks) - that provide consumers with assurance on minimum level of security.
- Industry to build services and products that are compliant to government cyber security benchmarks or standards. Especially IoT medical devices as these need specific safe guards in place and should adhere to mandatory cyber safety standards.
- Industry to build services and products that are designed with cyber security in mind to minimise exposure to cyber security threats (e.g. development of secure by design standards by the Australian Government).
- Support the establishment of standards for security testing which is comprehensive and considers 3rd party suppliers, culture, policy etc and not just the traditional penetration testing.

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

- Consideration to impact import and export of services and products.
- Development of a compliance criteria, standard process for specific goods and services can be considered, however consideration needs to be given to how this may adversely impact innovation and speed to market for services and goods.

Please also see responses to question 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?

The decision to safely devolve government functions to the private sector needs to be carefully considered and examined for unintended consequence and requires thorough consultation. Some functions simply require the government to drive the innovation or service while others may be better served by funding existing Australian based entities to drive innovation. Two cases to consider:

CySCA – The Australian Cyber Security Hacking challenge was driven by the initial 2016 Cyber Security strategy. The program successfully engaged students at universities and TAFEs across Australia in a national Capture The Flag (CTF) competition which was free from commercial influence and was supported by various industry partners such as Telstra, Microsoft, Cisco, CBA, HackLabs, Splunk, PwC, BAE Systems and the Australian Information Security Association (AISA) in conjunction with Government. All the entities either provided technology platforms, people resources, prizes or space for the event to occur nationally and at the Australian Cyber Conference in 2018. This event drove an agenda of training at all the education providers, uplifting hands on skills for the next generation and stimulated interest in the community helping to drive new talent into the sector. Due to a lack of funding and dependency on handouts from industry, the event was unable to run in 2019 to the major disappointment of hundreds of cyber security students across the country. Lessons learned from this are:

- To be successful the ACSC needs dedicated funding and resources to manage and coordinate events and programs.
- Education providers (universities and TAFE) positively adjusted their training to deliver real world hands on training and they trusted the government (no commercial agenda) hence the large student participation level.

- Winners of the competition also had an enhanced pathway to seek employment opportunities in government to help defend Australia.

CyRise – Australia's only dedicated cyber security start-up accelerator is funded by Deakin University and NTT. The joint venture has stimulated the cyber security start-up sector in Australia and conducts entrepreneur boot camp sessions and connects entrepreneurs to Australian organisations and venture capitalists. Over the last two years CyRise has built an excellent program and incubated a number of successful start-ups such as Cydarm, Netcrypt, Cynch, HackHunter, SecureStack, Dekko Secure, Scram Software and Detexian and is currently seeking the third round of entrepreneurs to participate in the program. With additional funding from government under a revised cyber security strategy, CyRise could dramatically expand their services and offering to build an even bigger ecosystem of innovation in Australia and attract international talent to our shores, helping to position our economy for the future.

Key CyRise achievements

- Over $500,000 invested into early stage cyber security startups.
- Most active cyber investor in Australia.
- Program participant awards include:
    - Securestack named one of the hottest startups on the globe at RSA in San Francisco
    - Dekko Secure awarded enterprise contract with NSW Police.
- 50 per cent of CyRise companies have raised external capital, which is at world class standard for an accelerator model.

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

Laws relating to critical infrastructure providers and telecommunication providers currently exist, but require some modification and clarification, particularly around the definition of critical infrastructure (CI).

CI are those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security. Some examples of critical infrastructure include essential services we all rely on in our daily lives, such as power, water, health, communications systems and banking. CI should be expanded to include major supporting areas in the supply chain and systems of national use, particularly cloud service providers like Amazon and Azure who under the current legislation definition would not be considered CI. For example, if all the four major banks use Amazon, then government should consider Amazon as part of the nation's critical infrastructure. It is also important that cloud providers are not overburdened with legislation, complicating and reducing their accessibility and value proposition in the Australian market as this would adversely impact to the competitiveness of Australian business using these providers to service customers on the global trade stage. A balance needs to be found to mitigate the national risk, while still being competitive as a place to do business and establish high tech start-ups. Cyber-physical systems like energy, water and manufacturing that support physical infrastructure, controlled by ICT, need to receive special attention while developing legislations. For example, with the increasing usage of IoT enabled appliances, demand response enabled devices, and installation of new monitoring units in the energy distribution networks, new dimensions are added to the cyber threat matrix, which require specific guidelines for cyber-physical systems.

New regulatory obligations set by APRA in CPS 234 have mandated standards of good practice for the financial services sector, but there are many industries that hold and process information that should have similar expectations defined. At roughly 1,000 data breaches reported in Australia annually, it is clear that more direct guidance is required.

While the legislative environment is not complete, it is also important to avoid the mistakes made by the current government around the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA) (e.g. minimal consultation in industry, negative impact to Australia's technology

sector, poor standing on a world stage and lack of appropriate judicial oversight) and Australia moving to agree to the USA CLOUD Act.

11 What specific market incentives or regulatory changes should Government consider?

- Tax breaks for organisations that meet the 'essential eight', definitions and road maps.
- Tax incentives to hire students and graduates to work in cyber security roles.
- Tax incentives to invest in cyber security R&D initiatives.
- Government accreditation such as a cyber security star rating system for goods and services.
- Enable a greater number of providers to access the small business cyber security grant to uplift small to medium businesses (e.g. for Managed Service Providers and universities to access the program which is currently only limited to the Council for Registered Ethical Security Testers (CREST) certified organisations). Cyber security is so much more than just a penetration or vulnerability test, it is mainly a people and process problem, hence culture and behaviour. The existing scheme was poorly designed and lessons from the failure should be reviewed to understand why the existing scheme failed to ensure a revised scheme delivers value to small business.
- Mandate that every company director should undertake some form of minimal cyber security training to improve awareness and understanding of cyber security risks.

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

For digital goods and services to have 'built in' cyber security features, reviewing and updating the cyber security guidelines in the presence of new cyber threats is essential. The guidelines need to consider the domain specific impacts of cyber threats across different layers of the ICT systems. The consequences of cyber attacks on physical devices should be incorporated and appropriately valued in developing the minimum cyber security standards for digital goods and services. A cyber security star rating will influence the manufacturers and service providers to design goods and services that have a minimum cyber security feature by default. Medical devices and life sustaining systems should be regulated just like baby car seats or the banking system.

Resilience, sustainability, adaptability and ***recovery*** of business and government functionality and activities is an ongoing challenge in a constantly evolving threat environment. It is essential not only to impart knowledge and build cyber-security awareness requirements within business elements, but also to identify and manage the risks effectively in terms of resilience, sustainability, adaptability and recovery as cyber-security settings and goals.

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

Research and guidance for secure software development particularly in the context of open source, agile and continuous integration/continuous delivery. Market forces should define supply chain management, however in some instances clear standards like APRA's CPS234 or frameworks may be required to drive change. Deakin recommends the government develops a standard industry minimum benchmark scheme that enables suppliers who are subject to CPS234, the ability to use the test results from the scheme as evidence of achieving a minimum verified security level. This would allow financial institutions to use the attestation and results derived from the scheme to satisfy their review and audit functions, reducing the need for each bank to undertake independent testing of the supplier multiple times. Hence, reducing the burden on the supplier.

Australian is home to a highly skilled population, particularly within the government space. Implementation of laws such as TOLA reduces trust within the Australian government to fulfil the privacy requirements of the population. Much of the supply chain is owned by businesses requiring partnerships between public

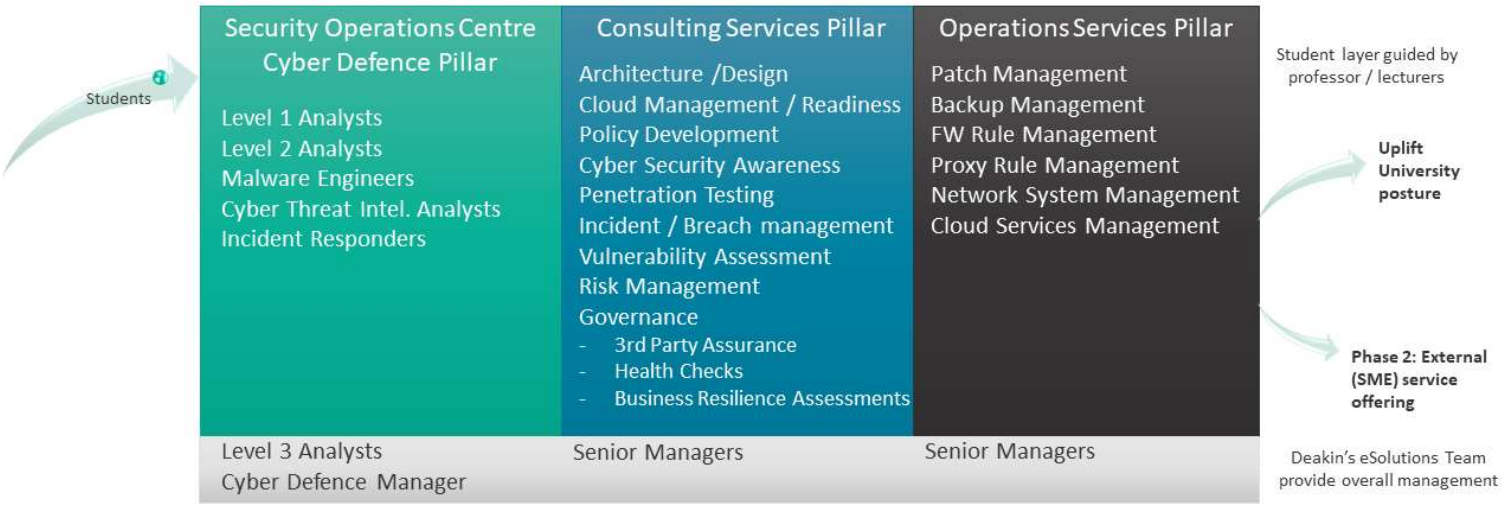
and private companies. Currently only perceived as a requirement for government agencies to adhere, the Protective Security Policy Framework (PSPF) and Information Security Manual (ISM) provide a means to address security gaps within private organisations. There is no direction or advice to business to comply with these controls, independent of their dealings with government. Promoting the implementation of these controls through lower cost recommendations or alternatives will begin to address this need. Cyber security leadership support to smaller businesses is not available or mandated. Responsible handling and storage of information and an accreditation standard for customers of those companies will provide consistency similar to the ANCAP or food safety ratings.

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

The Australian Government should build and run a centre that provides Security Operations Centre (SOC) functions plus consulting services and operations services at a whole of country level or state level (e.g. with nodes in each state). Universities and TAFE within each state can elect to participate in the program by supplying students and in some instances staff to help manage students and to learn themselves. Students could work for a minimum of three months in the environment to gain insights and expertise on solving and addressing real world problems.

Deakin is developing this concept as the Australian Cyber Protection Centre (ACPC) internally for Deakin students, however a model adopted at a whole of country level or state level would be beneficial to the nation:

- Significantly improve teaching quality by uplifting educators, lecturers and professors by exposing them to real business challenges.
- Improve student experience by enabling them to branch into SOC, consulting services (architecture, design, governance) and operational services. Not every student is suitable for a SOC role, however they may be suited to architecture, policy or governance.
- The model enables multi skilled pipeline development for the next generation workforce and provides a vanilla service to help uplift small to medium businesses, getting them familiar with cyber security and the related services and benefits. At some point these small businesses will understand the value and move to a more commercial model which provides a higher level of service. As a consequence, the proposed model also helps to increase the number of customers looking for Managed Security Service Provider (MSSP) services.
- There are research benefits from the program which will help improve threat telemetry and provide a greater understanding of the threat impact to Australia and small to medium businesses.
- Universities who join the program can also become customers, thereby increasing their internal cyber security maturity and capability.
- Industry can easily recruit talent under this model and it provides the Australian Signals Directorate (ASD) with a mechanism to identify special talents that might be relevant to protecting Australia at a national level.



Node Locations: Regional & Melbourne

Illustration of the model Deakin is building internally for Deakin cyber security students and staff.

Cyber security education should not be limited to technical aspects. Deakin University will release a Master of Cyber Security Leadership course, which will incorporate organisational psychology elements along with strategy, stakeholder management and crisis communications.

Higher education exemptions to study cyber security courses which are independently accredited by government (e.g. Australian Cyber Security Centre or ASD). In Victoria, TAFE Cert IV is free and has attracted large numbers of students, hence university courses should also be funded by the Government to boost the diversity and pipeline for the future. This could also be extended to the retraining of people being displaced by automation or who want to change careers.

While a number of activities can be undertaken to increase the number of Australian students in cyber security, the sector has a shortage of appropriately trained talent to teach cyber security across a range of disciplines. Reducing visa requirements to bring in external lecturers/professors/trainers from overseas would be beneficial to the sector. Deakin is drawing on talent directly from the sector (e.g. Adjunct Industry Professors) who have real world hands on experience. A longer term solution is for the government to promote a pathway to become a teacher/professor/trainer in cyber security.

Other suggestions include:

- Extend the Australian Defence Force (ADF) Gap Year programme to include cyber roles with the ADF.
- Revisit the Queensland ICT career streams framework to reflect better classification for the different cybersecurity job roles; and update the Skills Framework for the Information Age (SFIA) with the new and revised cybersecurity skill definitions.
- Build a program to attract ex-pats working overseas to return to Australia, bringing with them their international expertise.
- Create programs or provide incentives to retain top talent in Australia and prevent a brain drain as talent moves overseas. This may also require adjustments to legislations to keep new high tech businesses in Australia rather than creating an environment that pushes them to the USA, UK , Europe or other countries.

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

As with all insurance, if consumers do not see value they will not buy into a policy. The cyber insurance market is currently immature and subject to many variables which are often outside the control of both the

insurer and the consumer. For example, attribution of cyber crimes can be extremely difficult and the level of sophistication and resource available to cyber criminals will also vary greatly. A policy may cover losses arising from malware, but not if it is an attack originated from a nation state as it would be difficult for any organisation to adequately defend itself from a foreign government. Compliance is also not the answer as an organisation can be Payment Card Industry Data Security Standard (PCI DSS) compliant, but post the review may suffer a catastrophic data breach simply because compliance does not equal security.

In Australia the financial services sector has been an early leader to adopt insurance, but it often only covers the actual monetary loss from theft as opposed to the cost associated with remediation and compensation to customers.

The other aspect of cyber insurance is protection from litigation. For example, if a data breach occurs and personal customer data is stolen, would the organisation who suffered the data breach have an insurance policy that covers litigation from customers who subsequently suffer from identity theft? If we go down this path it may be a slippery slope, consuming the courts with civil litigations.

Clear Product Disclosure Statements (PDS) written in plain English should be available for cyber insurance. The current regime for cyber insurance is so complicated and opaque that cyber insurance policies exclude everything and prevent payout for legitimate claims. This is a global and domestic issue.

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

High volume, low-sophistication malicious activity targeting Australia could be reduced using a multi-pronged approach to implement a 'Clean Pipes' Australian ICT platform:

- ISP – black hole malicious sites hosting known malicious content (hence the concept of clean pipes). Consumers could opt in and out of the service which is provided at no additional cost as it is coordinated by the government (ASD / ACSC). The opt in and out feature is important to give consumers a sense of choice.
- Domain-based Message Authentication, Reporting & Conformance (DMARC) use by all government agencies (federal, state and local). Setting DMARC within the broader context of active defence – in the UK this includes the Exercise in a Box for organisations to test resilience and recovery plans, and software tools such as CyberChef and LME (Logging Made Easy) that have been released by NCSC on GitHub.
- Australian Government notifying the approximately 1.2 million households with insecure routers / modems how to better secure them.
- ISP – detecting malicious outbound connections (DDoS, Command and Control beaconing) to notify their customers and place them on a restricted network which limits the damage or network congestion to other customers.
- Eliminate spam voice telephony issues that currently target vulnerable members of society and interrupt both personal and professional activity.
- Awareness and behavioural change campaigns. Simple phishing training across the economy and community will have a major impact. We see the measurable impact within organisations who have conducted phishing awareness. Through one vendor, the average phishing susceptibility is reduced from greater than 25 per cent susceptibility prior to training to below 5 per cent within 12 months.

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

Please see response to question 16.
Additional information from the Australian Information Security Association indicates that 5 per cent of industry professionals believe a hostile environment is not possible to create or will adversely impact society, 95per cent believe the government should be taking a more proactive approach.

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

Improve two way communications using a standardised communication framework, with government taking on the role of coordinator of information.

Private individuals are faced with the challenge of not knowing if they are 'safe' online on a daily basis, not knowing if their devices are compromised or if a communication is legitimate. Certain segments are more vulnerable that others, which requires tailored response. However, a government-provided service that would answer the questions 'am I safe?' or 'is this legitimate?' could provide real value. The banking sector invests in advanced technologies to analyse endpoints for behaviour and communications for legitimacy. This type of advanced capability should be brought to the Australian community more generally, but would require significant planning and investment.

The government could kick off projects with various universities to conduct research to identify various threats, develop frameworks and test various recommendations to determine what works best for the various sectors. For example, what works best for banking may not be appropriate for the education or health care sectors.

The Australian government via ACSC could also implement an application that can be used by various organisations, similar to a tsunami warning system, but for cyber security. Under this concept, organisations can subscribe themselves based on their sector, provide information on the number of staff dedicated to cyber security, list their position in the organisation and then receive custom push notifications that are specific to their sector. Under this system the government could also ask permission to scan the external interface of the organisation (e.g. opt in) which would then enable the government to have a more proactive approach to defending organisations without necessarily imposing additional legislative changes. Under this system executives on boards could receive messaging tailored to their level, while technical staff could receive information on the technical threat and suggested mitigation strategies. The app could also be used as an education channel to Australians who subscribe.

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

- Cloud based services that are used by major organisations.
- Health care networks.
- University networks.

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 like the Cyber Security Small Business Program which was limited to CREST should be opened up to allow universities to help small to medium businesses and authorised managed service providers like Telstra, Optus, NTT and CyberCX.

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

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

- Improved security clearance procedures to offer faster service and to build a pipeline of multi classification workforce which can be enacted on short notice.

- Additional resources within ACSC to deal with the challenges as more business and citizens are impacted by cyber threats.
- Mechanisms in place to help retain talent within ACSC (non-contract) and reduce the loss of talent to industry (i.e. reduce the attrition rate).
- The government should publish clear guidelines, available through and via the ACSC for reporting vulnerabilities through to government. Specifically, KPI's for reporting zero day vulnerabilities uncovered within government back to the ACSC.
- Populate the Joint Cyber Security Centre (JCSC) in the major capital cities with people who have a broad range of skills to provide more value to the community, businesses and academia.
- Enable paid placement of Australian students into the JCSC to help uplift services and build a talent pipeline.

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

Deakin University agrees that a lack of cyber awareness drives poor consumer choices and subsequently market offerings. Branding or a cyber mark similar to the energy star rating system may drive consumers to make the right decisions. However, consumers are often driven by price, therefore the system needs to demonstrate a dollar value comparison to be effective. Hence, the higher the rating the less monetary impact the consumer will have. If this cannot be achieved, then consumers will not see a correlation between the benefits of selecting a more expensive and more secure item which is cheaper long-term (reduced risk) compared with a cheaper less secure item (more expensive to maintain and will lead to a high risk of data loss long-term).

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

The balance between safety and availability: Within the specific context of healthcare, it is generally accepted that digitisation efforts such as the Electronic Medical Records (EMR) systems provide significant benefit, empowering better health outcomes for patients. There is a delicate cost-utility function involved in balancing the security of such data against the potential good that can come from offering availability for such data to be used for research and industry. The benefits of such availability can manifest in improving healthcare for patients, as well as economic competitiveness for Australian businesses. Hence, we advocate for representation in cyber security policy planning committees to support such interests.

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

Changing the public perception of cyber security to cyber safety: We posit that a shift in the tone and messaging of cyber security toward a positive call to arms message of 'Cyber Safety: protecting your loved ones and wellbeing,' will enjoy greater palatability across cyber vulnerable communities, such as the youth, elderly and marginalised groups. The cyber safety message aligns with the Australian egalitarian outlook and empowers individuals toward a positive outcome of protecting their loved ones.

Consumer, youth and elderly generation campaigns: Cyber security threats can manifest in different formats, contexts, and threat vectors specific to different demographic groups and social communities. In addition to this, different addressable cohort segments require tailored messaging and usage contexts to make cyber safety actionable and relevant to resonate with them. We posit that tailored campaigns will enable and improve cyber safety awareness and education.

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

Yes, seeing cyber security features prioritised in products and services will achieve the following:

- Drive organisations to start including cyber security by design.
- Increase awareness by being more visible – it may not drive the right consumer behaviour initially, but it will start to raise interest, provide a point of comparison and will eventually lead to behavioural choices if it is branded correctly.

An important aspect to consider is that the value proposition of security is not relatable to most people, hence it needs to be developed in a way that resonates with the target addressable market.

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

- Long term planning for five to ten year horizon with review points every two years to assess or adjust focus – with committed (ring fenced) cyber funding to assist government agencies.
- Bipartisan approach to the cyber security strategy – we need a strategy that will survive a change in government.
- A cyber security strategy which has measurable, data based outcomes that can be tracked, validated and measured.
- The previous strategy was reviewed after the first year and then lacked subsequent reviews that were publicly published to show how we are tracking as a country.
- A lot of the funding under the previous strategy was tied up in relocation of staff and mergers of departments without any real focus on building capacity and sustainable resources.
- More needs to be done to stimulate innovation and a vibrant technology sector that can be measured and assessed.
- There needs to be improved coordination between all three levels of government (federal, state and local council) to remove duplication and competitive programs so Australians get the best value for the level of expenditure. For example, why do states and territories have very different cyber security strategies that do not incorporate the larger national agenda?
- Local councils in Australia promote poor cyber behaviour online using third party services that email billing notices that look very much like a scam. Hence they are reinforcing bad behaviour and need to move to systems similar to the MyGov platform or at least a provider that includes the council's domain in the URL.
- To help develop and incentivise research in cyber security, the government should support the proposed definitions of the new cyber security FOR (Field of Research) codes. This will allow researchers to have accurate categorisation of their research efforts in the cyber security discipline and will help the discipline stand out at the forefront of national strategic priorities.
- Investment in cyber security research should not be limited to just the Cyber Security CRC which has limited themes, but be opened up to encompass a greater range of researchers from across a number of other domains such as humanities, psychology and business. Also greater participation of industry is required to drive the outcomes needed by government and the various industry sectors, including retail, legal, healthcare, mining, manufacturing, energy and education.
- A national cyber curriculum from primary school. Developed in consultation with the higher education sector and industry.
- Harmonisation of legislation on a domestic and international scale to enable Australian organisations to focus on an aligned set of requirements as opposed to juggling numerous and sometimes conflicting expectations. This enables Australian organisations to build stronger practices with their finite resources.
- The 2016 strategy was constructed and guided by a very small group of experts from limited sectors. It is highly recommended that a broader and more diverse group of CIO / CISO / CSOs from industry, academia and the Australian Information Security Association (AISA) be actively involved as experts in the development of the 2020 strategy. Deakin has the largest and most comprehensive Executive

Advisory Board for Cyber (EABC) in Australia and would be happy to assist the government. The EABC is comprised of 39 executives from across industry and some government agencies.

- Establish a clear and concise federal government charter of responsibilities to define what, when and where government responsibility will start and end and where the commercial sector will step in.
- Clear remit for government funded entities established. AusCyber, ANAO, ACSC, AusCERT. Ensure that overlap is reduced and efficiencies are achieved. Remove commercial conflicts between the ACSC and industry.
- With the recent growth in Australian security agencies' reliance on cyber capabilities and drones, Australia should develop better means to secure algorithmic fairness and data integrity, as well as to ensure that these new methods are communicated properly to the public. The impact of these new cyber capabilities on civil-military relations should also be further considered.
- Cyber is now of such critical importance that it should receive the same consideration by governments as other risk area where appropriate regulations apply, such as workplace health and safety, corporation's law and trade practices
- Every company, institution and level of government should have a security strategy. To achieve this the government needs to develop toolkits and templates organisations can use and adopt to uplift their security posture to defined levels.

Deakin University contributors:

Mohamed Abdelrazek – Associate Professor
Aman Maung Than Oo – Head of School Engineering
Shama Islam – Lecturer in Electrical Engineering
Andrew Cain – Associate Head of School (IT)
Jesse McMeikan – Manager Industry Projects
Leonard Hoon – Senior Research Fellow
Matthew Warren – Deputy Director CSRI and Professor
Zubair Baig – Senior Lecturer Cyber Security
Amani Ibrahim – Senior Lecturer, Cyber Security
Shiri Krebs - Senior Lecturer, Business and Law
Chang-Tsun Li - Professor Cyber Security and Director of Research for Deakin's CSRI
Fadi AlJafari - Information Security & Risk Manager, eSolutions
Damien Manuel – Director Cyber Security Research and Innovation (CSRI)

Deakin University partner contributors:

James Kotsias - Cyber Technology Research Manager Security Domain, ANZ
David Fairman – Chief Security Officer
Kathryn Manuel – Digital Security Officer
Nigel Hedges - Head of Information Security, CPA Australia
Leonard Kleinman - Chief Cyber Security Advisor (APJ and EMEA), RSA International
Shannon Lane - Chief Strategy Officer, Shearwater Solutions
Craig Templeton - CISO & GM Group Technology Platforms at REA Group
Julian Fay – Chief Technology Officer, Senetas
Andrew Wilson – Chief Executive Officer, Senetas
Simon Galbally – Chief Marketing Officer, Senetas
Ben Parkinson – Chief Information Security Advisor - Federal Government, SecureWorx
Scott Handsaker - Chief Executive Officer, CyRise
Adam Hergert - Executive Security Consultant
Abbas Kudrati - Chief Cyber Security Advisor (Austraila,SE Asia,India), Microsoft