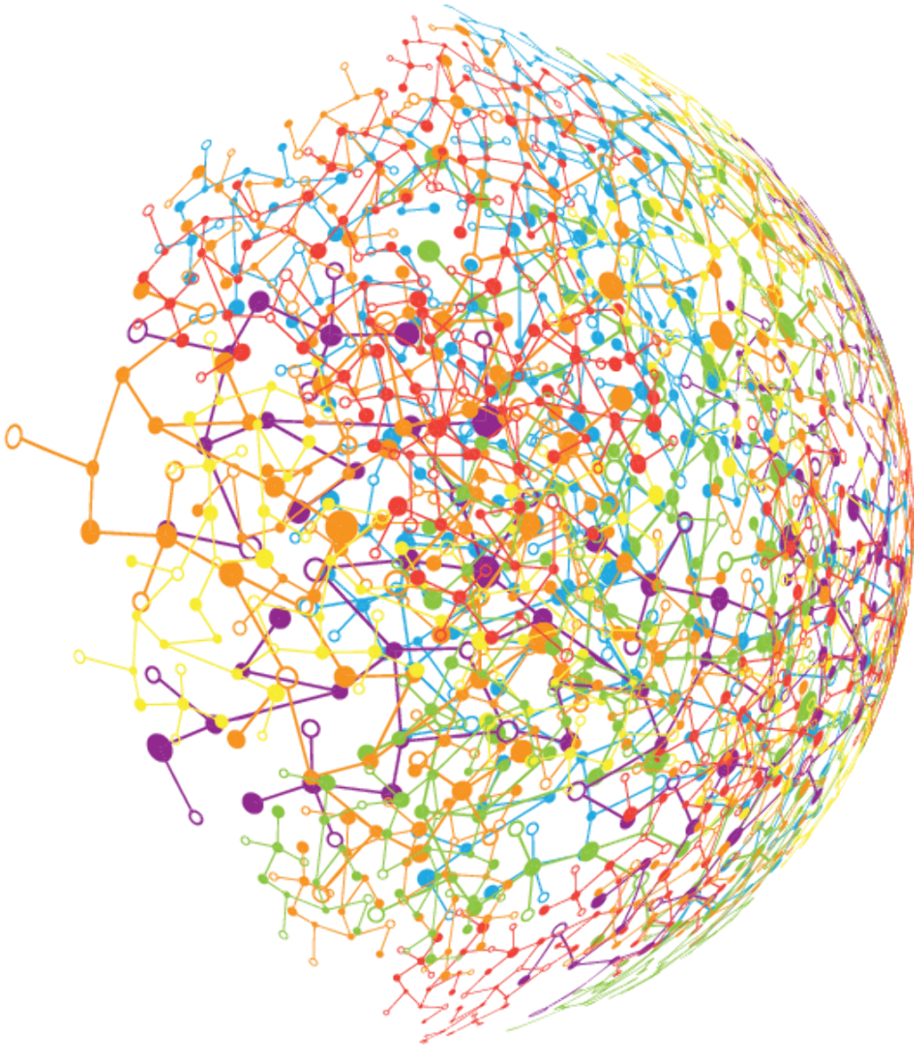
Deloitte.



Australia's 2020 Cyber Security Strategy: A call for views

Deloitte Submission

November 2019

Contents

Executive Summary

Deloitte is pleased to provide a submission to the Australia's 2020 Cybersecurity Strategy update. Cyber security is a complex, multi-disciplinary and ecosystem challenge globally but it also represents an opportunity to develop Australia's cybersecurity ecosystem and potentially provide a burgeoning export opportunity.

Australian citizens and businesses rely on the internet for their essential work and home services. Threats to the internet will have broad reaching affects and cybersecurity and cyber resilience will enable internet services to function and Australian citizens and businesses to continue to prosper. An upcoming 2019 Deloitte Access Economic report will show that as part of an APAC region, improving our cyber preparedness could increase APAC GDP by $287bn. Australian businesses are in a prime position to take advantage of this as organisations who are more certain of cyber risks being managed appropriately are more willing to embrace productivity and potentially will invest more in technology. Overall this will improve productivity and decrease risk aversion.

It's our view that Government must play a pivotal role in cyber preparedness and building a cyber-resilient ecosystem. Initiatives such as Australian Cyber Security Centre (ACSC), Joint Cyber Security Centres (JCSC), AustCyber, Cyber CRC's are helping Australia improve it's cybersecurity resiliency but also create a burgeoning export market for cybersecurity services. The Australian Government taking a strong leadership position for cybersecurity regulation and helping to harmonise regulation across the APAC region will give Australian businesses more confidence as they look to improve productivity.

We look forward to the final strategy update and would welcome feedback on our submission.

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

Australia, as a technologically advanced society is at risk from an evolving number of threat actors and scenarios.

Australian Public: As the Australian public becomes more technology literate and technology use flourishes, a basic lack of cyber knowledge is a critical threat, with the general public (particularly certain segments) likely to fall victim to commonplace and easy to spot cyber threats. Education and awareness campaigns run by government will assist in mitigating this threat. A baseline of national security knowledge should be aimed for, focussing on minimising the number of potential targets. The consumer goods industry is of particular concern for Australian citizens as organisations grow to hold more of their data in many forms, with information technology (IT), operational technology (OT) and products converging e.g. health information from pacemakers and wearables[1].

Enterprise: The increasing levels of attacks on large scale enterprises and resultant impacts to these businesses and their customers can cause significant harm to Australia's economy. Regulations such as the CPS 234 are examples of good practice by government in ensuring financial sector organisations maintain a baseline level of information security, protecting Australian businesses and the public[2].

State: Threats to government are also a point of concern. The involvement of state actors with large scale offensive capability can pose a threat to the democratic process, and harm may come from the release of sensitive information, particularly information involved in Australia's national security and military efforts.

IT & OT: Increasing interconnectivity in all industries has led to an increase in connected sensors and devices that transmit, store and process data. Each device that is connected increases the potential vulnerabilities an organisation faces and the surface area that needs to be protected [3]. Infrastructure and OT technologies are increasingly converging yet are often poorly secured due to technical limitations and the additional complexity brought into play by the use of physical components. Legacy technologies and interfaces with SCADA and/or other systems make it difficult for organisations to react quickly to threats, with unpatched systems leaving them vulnerable to threats that could otherwise be easily mitigated. Government should increase its focus on these infrastructure and OT organisations, such as Energy[4], Transport and Healthcare to ensure that a baseline level of security is maintained in these industries.

[1] https://www2.deloitte.com/us/en/insights/topics/risk-management/cyber-security-threats.html
[2] https://www2.deloitte.com/au/en/pages/risk/articles/apra-cps-234.html
[3] https://www2.deloitte.com/us/en/insights/topics/risk-management/cyber-security-threats.html
[4] https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/cyber-risk-electric-power-sector.html?icid=dcom_promo_featured|au;en

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

The management of cyber risks in the economy at present lies at heart in three areas: end-users, providers and government. However, end-users in today's economy unfairly bear risks in products and services that they acquire. There should be greater input from the Federal government on practices required to look after the interests of Australian citizens. This should entail an expectation that government are doing what they can to protect citizen data.

Cyber Security should be the responsibility of the Government, Businesses and Citizens alike. Nevertheless, citizens and businesses both large and small will invariably turn to the Australian government for guidance, advice and leadership. As with policing and national security, the Australian Government should be responsible for setting laws and policies, and businesses and citizens should have been provided with resources necessary to protect themselves and to assist with remediating any cyber crimes or attacks that occur to them.

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

End users need to be empowered with enough information and knowledge to allow them to make informed decisions. In particular, end-users must be made aware of the steps that a service provider takes to protect their data, assets, and information, and the controls that are in place to mitigate cyber risks e.g. DDoS mitigation services.

Goods and services providers should have a responsibility to ensure a high standard of cyber security exists in their organisation and in the goods/services they provide. As these organisations have more capital and know-how than end users, their appropriate maintenance of cyber security resilience should be the first line of defence from cyber attack. Critical systems providers such as telecommunications, transport and energy should be held to even higher standards and remain accountable for cyber attacks that impact their end users.

Goods and services providers must also be transparent to enable end users to make informed decisions. Whilst service providers usually make such information available, they should make a firmer attempt to provide this information to consumers at the point when the consumer makes the decision to consume their product / service. This information should also be in an easy to digest form; e.g. via a cyber security rating out of 5 stars. Consumers often make decisions within a bounded length of time and a ratings system would give clarity to their decision making. It is important to avoid long reports that are difficult and tedious to read.

Government should maintain its oversight function in cyber security. Government's role as a facilitator of cyber security development and information sharing should be a focus, enabling organisations across industry sectors to share critical cyber information. On the global stage, the Australian government should consider collaboration across borders, particularly with countries that sustain regular, focussed attacks so that best practice techniques and funding models can be emulated at home.

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

Governments should focus on maintaining a policing function for addressing the most serious threats. These threats include nation states and sophisticated criminal groups attacking Australian organisations.

A clear accountable body in the government for cyber security should hold the ultimate authority for maintaining national cyber security, while providing appropriate regulations, specialised skills and knowledge and general oversight.

The Government's role in protecting organisations from serious threats should also be clearly defined. Critical infrastructure organisations which are crucial to the maintenance of the health, safety and wellbeing of Australians should retain primary responsibility for maintaining appropriate cyber security practices but should also have the backing of the government's cyber security capabilities (e.g., in areas such as incident response). Government should provide a framework but should not be directly responsible for managing the security of private sector businesses.

A focus on strong regulations and the uplift of cyber capabilities, driven by government in critical infrastructure industries, is another key role government can play. The rigor of the regulation and the levels of compliance to be applied should be based on a consideration of the level of security that is required according to the threats that industries face. There should be coordination between the federal and state governments to consolidate and provide a single unified approach.

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

To build and maintain trust with the community, the Australian Government should be proactive and seen to be proactive, while also being open and transparent without compromising national security, capability or operations. Openness and honesty from Government on security practices and methodologies, and their usefulness to the public, is vital to earning trust. Collaboration and information sharing should be facilitated between organisations and industries, and between agencies.

Resources should be prioritised to enable the capabilities to be well supported. The Government should ensure that it has the cyber capabilities that can protect the nation from today's threats now and invest in next-level capabilities that can protect it from threats that might emerge in the future. This means that national programs and initiatives – such as My Health Records and Open Banking – should be supported by frameworks that are secure, vigilant and resilient.[5] Cyber risks should be considered as a strategic imperative by agencies and organisations.

[5] https://www2.deloitte.com/au/en/pages/risk/articles/take-lead-cyber-risk.html

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

Assurances provided through warranties or safety ratings for digital products and services should be developed to help protect consumers and inform their choices in the competitive marketplace.

Warranties can be provided for digital goods and services to provide a guarantee of a certain level of protection. Technology providers have gone to market with cyber warranty for technology products, such as endpoint detection solutions, to guarantee a level of protection against a particular threat, such as ransomware. The warranty provides a minimum level of guarantee for the product or service and indemnifies the customer if the solution is not able to provide the agreed-upon protection in the event of an incident.

The protection of consumers' public welfare has been part of the government's responsibility in many industries, such as food and medicine, so as to inform consumers and provide them with assurance on the quality and safety of goods and services. For example, ANCAP Safety Ratings are provided for motor vehicles and are graded between 0 to 5 stars to indicate the level of safety of the vehicle in the event of an accident, based on the effect an accident is likely to have on the vehicle and the ability of the vehicle to minimise the effects of that accident. Similarly, an Energy Rating is provided for electronic appliances to indicate the energy efficiency and help identify the energy consumption of the product. In many instances, the ratings are international or national standards and labelling of the rating is mandated for certain products.

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

The Federal Government and industry can support the security of consumers through a two-fold approach. First, they can work together to continue promote cyber security awareness. In doing so, government should also consider funding for education in cyber security and broader STEM, in order to build a national workforce of people better able to help respond to cyber risks. This funding will assist younger generations in being aware of cyber risks and cyber safety. Second, a framework should be developed that enables businesses and consumers to engage in a secure environment across Australia.

Government and industry can support the cyber security of consumers by working together to focus on the human element to bring deep expertise and a strategic perspective to cyber security. Strategic initiatives should be coordinated to further the development of skills and expertise, foster common standards and approaches and support information sharing.[6] Cyber security strategy means nothing without the skills and talent needed to execute it.[7] While tools and software leveraged for cyber security can help organisations do more with less, they are not an adequate substitute for human expertise, which can often detect anomalies and threats that software programs alone would otherwise miss.[8]

There is room for Government and industry to work together and collaborate, such as through wargaming exercises for executive and leadership teams. Wargaming exercises are simulation exercises that immerse participants in a simulated and interactive cyber threat and attack scenario. These exercises can help develop awareness of potential threat vectors and prepare agencies and organisations to respond to incidents and breaches when they do occur.[9] It is important for agencies and organisations to not only be able to put their incident response playbooks into practice when threats emerge but to also develop the ability to exercise sound judgment when faced with unknown threats and types of incidents that are not scripted within playbooks.

[6] https://www2.deloitte.com/au/en/pages/financial-services/articles/cyber-regulation-asia-pacific.html
[7] https://www2.deloitte.com/tr/en/pages/risk/articles/protecting-sensitive-data-government-cybersecurity.html
[8] https://www2.deloitte.com/au/en/pages/risk/articles/take-lead-cyber-risk.html
[9] https://www2.deloitte.com/us/en/pages/risk/articles/cyber-risk-services-cyber-war-gaming.html

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

Government and industry should develop a working partnership that encourages innovation while maintaining a balance with considered rules in order to develop cyber security quality within Australia.

A key model to consider is one of co-investment. Co-investment in new, secure technologies that increase cyber security capabilities should be encouraged and actively funded in partnership between government and industry, incentivising the development and dissemination of such technologies.

Government and industry can also work together to cultivate innovative mindsets and enable security development by upskilling the next generation of cyber professionals. Encouraging a culture of information sharing and collaboration in cyber security research development is critical to fostering cutting edge security innovation. Joint events, such as cyber security conferences and security exercises, can be co-sponsored between industry and government to enable the sharing of technology insights across the public-private relationship, with strengths pooled to focus innovation.

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

Government's role as an overseer should be at forefront of cyber in Australia. In this, the development and enforcement of strong and sound regulation and cyber security guardrails is critical. Cyber security certifications, including for compliance with regulations, can however be safely devolved to the private sector. Government certified organisations can perform the assurance tasks of government, providing a large increase in certifying capability (resourcing) while allowing government to maintain its oversight function.

Training is another area that could be safely devolved to the private sector. This could lead to more targeted, efficient and attractive training and education programs. Government grants for the development of quality cyber education courses and accreditations could be invested into the broader community, such as the successful program at Box Hill.

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

Currently, there are no general regulations for cyber security. The regulatory environment is made up of industry-specific regulations and guidelines, such as the Australian Prudential Regulation Authority's CPS 234, the Australian Energy Sector Cyber Security Framework, Telecommunications Act 1997 (Cth), and My Health Records Act 2012 (Cth). Furthermore, there are additional provisions within the Privacy Act 1988, Cybercrime Act 2001 and Telecommunications (Interception and Access) Act 1979 (Cth), which relate to cyber security to differing extents.

Furthermore, the regulatory environment is steering towards a differing regulatory approach to the public and private sectors. And there currently aren't a broader set of standards in the government's framework that apply to both federal and state government.

Consideration of a harmonised approach to cyber security regulation is required, with provisions put in place for consideration of compliance against one standard in place of other, similar standards as compliant, allowing organisations to focus on maintaining information security, rather than information security as a compliance exercise.

Enforcement is dealt with by multiple regulatory bodies that have differing touchpoints with cyber issues, with each agency and regulatory body having varying enforcement priorities, functions and powers. For example, the Australian Crime Commission and Australian Federal Police may deal with cybercrimes, while the Office of Australian Information Commissioner may deal with breaches involving personal information. As different agencies are responsible for different issues, the penalties may vary significantly and be disproportionate. For example, the OAIC can seek penalties of up to $2.1m for breaches of the Privacy Act, which only covers personal information, but there is a gap for system breaches that do not involve personal information but may still affect the Australian community and businesses through issues such as operational disruption. It is important not only for regulatory reform, but also to provide enforcement bodies with the means to enforce the regulations in a consistent and meaningful way.

There is limited regulatory coverage for areas outside of critical infrastructure. While it may not be appropriate for a prescriptive cyber security law to provide overarching coverage of all businesses in Australia, there should be a minimum standard expected from businesses across all industries. By way of example, in the Office of the Australian Information Commissioner's 12-month Insights Report on the Notifiable Data Breach Scheme, the education industry placed within the top-5 sectors for sources of notifiable breaches. The education sector is not subject to its own sector-specific information security regulation or standard, which means there is a gap in coverage for breaches, notifiable or not, that occur to organisations within that sector. This is particularly a concern given the number of high-profile breaches at tertiary education institutions over the last 24 months.

Cyber risk should be treated as a priority at the board-level. This could be achieved by placing more focus on the Australian Securities and Investments Commission to ensure directors of companies are dealing with cyber risks and threats appropriately and in accordance with the Corporations Act 2001 (Cth).

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

Rewarding good cyber security practice should be an aim of government. For example, appropriate tax incentives such as the Research and Development tax incentive [10] will encourage investment in developing cyber security capabilities, equipping organisations with cyber capabilities and uplifting security nationally. Incentives like these have been previously suggested in the US as a method for improving cybersecurity through the public-private partnership [11], and are now implemented in the US state of Maryland[12] and New York City[13]. Other incentives to consider include good cyber security as a requirement for the awarding of government contracts and the provision of grants to small businesses for bolstering their cyber security practice.

The UK model for fostering home-grown cyber talent as a strategic vision could be similarly followed in Australia to ensure that the necessary investments are made into developing the cyber fundamentals and knowledge amongst the next generation of cyber professionals. There should be a focus on incentivising education institutions that develop cyber security courses and organisations that recruit local talent.

[10] https://www.ato.gov.au/Business/Research-and-development-tax-incentive/
[11] https://www.cdt.org/files/pdfs/20110308_cbyersec_paper.pdf
[12] https://www.forbes.com/sites/realspin/2015/09/23/cybersecurity-is-expensive-thats-why-we-should-offer-tax-incentives/#2f0b55175483
[13] https://www.accountingtoday.com/opinion/its-time-for-the-federal-government-to-incentivize-cybersecurity

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

Organisational and technical measures should be implemented by an organisation to ensure that digital transformation projects and product developments have the right security specifications and configurations.

The human factor remains a weak-link in agencies and organisations, and the industrial workforce needs to be upskilled to be able to design and deliver secure products and services to the market. To achieve this, awareness and cultural change should be a focus of Government to ensure that industry are delivering digital products and services that are built and delivered with security front-of-mind.

It is important to balance swift innovation and functionality with cyber security. It should not be an afterthought but a consideration throughout the end-to-end development lifecycle of applications and infrastructure, so as to minimise vulnerabilities and flaws in the systems that underpin the products and services in the market.

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

In the modern marketplace driven by data, the transfer of data is becoming more commonplace as data moves in, out and through supply chains and different ICT environments across the world. This provides greater risk exposure to threats as it becomes more difficult to understand where the data actually sits, particularly from a consumer's perspective. To build more trust and provide greater protection, consumers should be provided with more control throughout the lifecycle of data. Australian consumers will begin to experience more control of their data than ever before with initiatives like the Consumer Data Right legislation, which means that it will be more important to ensure that businesses are maintaining the utmost trust with their customers so that they can retain business. This involves being transparent with how consumer data is collected, used and protected throughout the supply chain, and should be an imperative on businesses as part of their supply chain management practices. Better and increased trust could be promoted through a greater focus on consumer experience.[14]

The availability of critical services can be affected through supply chains, as has been evidenced in operational technology environments, and in particular infrastructure used to supply the power sector. Emerging threats to supply chain and industrial control systems have made recent headlines, where cyberattacks were found to have originated from within the supply chain to impact the power sector, two of which targeted industrial control systems, and one which targeted IT systems.[15]

The Government could work towards creating standards for third party supplier assessments so as to lift the quality of services provided throughout the ICT supply chain. Verifications of compliance and the need for independent assessments could be enforced to ensure even greater assurance over and trust in providers involved in the supply chain.

[14] https://www2.deloitte.com/au/en/blog/risk-advisory-blog/2019/customer-experience-insight.html
[15] https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/cyber-risk-electric-power-sector.html

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

Governments and private entities can work to build a market of cyber security professionals by encouraging active cyber security learning throughout the educational experience, and into professional careers [16].

Government investment can foster the building of cyber security capability at a rapid pace. Areas that can be considered include government support for student work placements into cyber security areas, investment support for cyber security recruitment and the encouragement of immigration for skilled cyber security professionals.

Investing in education at all levels will be integral to filling the 17,600-person gap projected for 2026. At lower levels, primary school and secondary school IT programs should include mandatory cyber security components, introducing concepts and developing interest in cyber security in students. This will help to develop future end-user judgement skills and raise Australia's cyber literacy as these students move into the workforce. At a tertiary level, increased funding to universities for the development of cyber security programs and research will help to equip future cyber security professionals with a deeper level of understanding of cyber security concepts, too often missing from today's workplace due to a lack of tertiary courses focussed on cyber security.

Industry may look to develop cyber security professionals today by looking to the broader pool of STEM graduates, particularly those coming from computer science, IT and engineering backgrounds as these are typically highly adaptable to learning new technical skills and can become valuable assets. Getting these graduates to move outside of traditional roles for their careers (developers, software engineers etc.) to developing cyber security solutions can be especially fruitful. Casting the field further to non-STEM graduates also will give a source of cyber security capability, particularly in strategic and advisory areas that rely on business acumen and non-technical expertise.

[16] https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aoda-en.pdf

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

Cyber insurance has been available, but not widely used in some form for 19 years[17]. Globally, cyber insurance has strong uptake in certain countries, such as the US.

A key barrier to cyber insurance in Australia has been a lack of understanding regarding the use of cyber insurance and awareness of product offerings in the market. A large component of this is difficulty in understanding the benefit in investing in cyber insurance, noting the difficulty in quantifying the cost of a cyber incident and questions around the applicability of insurance to incidents that occur in the supply chain. Terms need to be clearer on what is and isn't covered as part of these insurance policies.

Insurance serves to provide protection to tangible events with quantifiable costs rather that intangible events. There is a currently a lot of grey area, with a lack of tried and tested cases to act as precedence relating to liability, costs, and other factors that go towards informing insurance premiums and payouts. Traditional insurance products for medical and property have been tried and tested in the market for many years, which is an opportunity the cyber insurance area has not yet been afforded.

Insurers need to develop expertise in cyber risk in order to appropriately provide insurance. Development of cyber risk knowledge in insurance brokers is a meaningful first step to developing sound cyber insurance policies. Considering cyber insurance in the framework of different types of insurance risk such as selection, parameter and pricing risk may help insurers develop their cyber insurance portfolios[18] and articulate their cyber insurance offering to the market. Insurers can consider insurance risks such as fraud risk (identification and proof of cyber incidents) in the development of their insurance offerings and develop innovative solutions to answer the questions posed by this; an example being the development of forensics based on blockchain technologies.

[17] https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-cyber-insurance.pdf
[18] https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-cyber-insurance.pdf

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

High volume, low sophistication malicious activity targeting Australia will inevitably increase. Whilst technical measures such as the blocking of communications are worth considering, they are difficult to execute in practice; technology typically remains one step behind any evolving cyber threat, even those of low sophistication.

A complementary approach is one of providing end users with enhanced decision-making skills at the point of interaction with the threat environment, therein decreasing the potential impact of threat scenarios such as WannaCry.

In order to do this, continued investment should be made in developing a strong cyber security aware culture in Australia by campaigning to increasing the awareness of cyber threats by the general public (particularly in more susceptible sectors of internet users). This strengthens the 'human firewall' and can limit the propagation of low sophistication attacks. The importance of cyber should be elevated and made comparable to that of work safety in organisations.

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

A vital deterrent for malicious cyber actors is the threat of pursuit by law enforcement should they perpetrate a cyber attack. Government should provide sufficient resourcing to pursue particular cases and be able to impose penalties (financial) on perpetrators.

Further enhancement of technical Australian cyber security capability will also help to foster a hostile environment for malicious cyber actors. Continued focus on cyber security research, collaboration with centres of excellence globally, and a focus on ensuring cyber intelligence information is up to date and relevant will all help to protect Australia's information and its residents.

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

Government and private entities can work to proactively remediate cyber risks on private networks by ensuring that information is shared proactively amongst actors in those services. Increasing incidence of information sharing is imperative to boosting industry capabilities, providing businesses (particularly smaller players) with more robust information, and a combined ability to gather, analyse, coordinate responses and communicate cyber security data[19,20]. An example of information sharing facilitated by government is the development of a register for cyber attack reporting, curated and managed by appropriate government agencies.

[19] https://www2.deloitte.com/content/dam/insights/us/articles/4921_Managing-cyber-risk-Electric-energy/DI_Managing-cyber-risk.pdf
[20] https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-thought-leadership-noexp.pdf

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

Critical systems that require robust cyber defence are numerous. Systems involved in delivery of essential services require particularly strong cyber defence.

Essential areas that should be considered for increased investment in cyber defence are related to services necessary to the public, such as healthcare, transport, electricity, telecommunications, military and fuel supply. Healthcare organisations, including health providers and medical technology developers are being increasingly targeted by cyber attacks on a global scale[21,22,23,24]. Attacks may cause significant difficulties in the provision of health care, with recent events causing delays in surgery in Victoria[25] and all non-emergency patients needing to be turned away from particular hospitals in the US[26].

Education is another target for cyber attack. Attacks on higher education can be particularly harmful, first due to the large amounts of personal information they hold, including student and research staff information. Universities also house significant amounts of research data, much of which is proprietary and sensitive in nature with potential uses in military and other significant areas[27].

[21] https://www2.deloitte.com/nl/nl/pages/life-sciences-en-gezondheidszorg/articles/cyber-attacks-in-the-health-care-industry.html
[22] https://www2.deloitte.com/us/en/insights/industry/health-care/value-of-cybersecurity-life-sciences-health-care.html
[23] https://www2.deloitte.com/ch/en/pages/risk/articles/medical-devices-cybersecurity-vulnerable.html
[24] https://www2.deloitte.com/us/en/pages/public-sector/articles/health-care-cyber-security-fraud.html
[25] https://www.theage.com.au/national/victoria/surgeries-delayed-and-patient-security-fears-after-cyber-attack-on-victorian-hospitals-20191001-p52wp1.html
[26] https://time.com/5690814/alabama-hospitals-ransomware-attack/
[27] https://www2.deloitte.com/us/en/insights/industry/public-sector/cybersecurity-on-higher-education-leadership-agenda.html

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

Government should consider co-investment and venture capital type investments for businesses that provide capability for additional protections to be provided to the community.
An equity co-investment is a minority investment made directly into an organisation in conjunction with another investor, e.g. venture capital firm. These can benefit government by lowering the level of upfront outlay required and can allow government to leverage the connections and knowledge of professional venture capital firms in directing its investments.

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

One of the barriers between sharing between government and industry is a fear of punishment arising from sharing information that may be unfavourable for the organisation, and thus penalties/legal consequences applied.

Applications of government protections for organisations that share information, such as exemptions from penalties, would increase the instances of sharing between organisations.

Another boundary is a lack of clear guidance regarding what types of information are useful for sharing between Government and industry. Clear guidelines to the types of information that should be shared, as highlighted by the World Economic Forum can be used (technical security measures, best practices, tools, techniques and procedures and indicators of compromise)[28].

[28] http://www3.weforum.org/docs/WEF_Guidance_Cybercrime_report_2017.pdf

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

We agree that a lack of cyber awareness often drives poor consumer choices and market offerings, but we would add that the main driver is usually consumer obliviousness to cyber risks, born of the feeling that incidents will not happen to them.

An appreciation for appropriate cyber security is difficult to come by naturally due to the lack of awareness of and transparency over how secure products and services actually are. In effect, an information asymmetry exists as businesses are afforded more awareness of the product and system design than consumers, which may provide providers with significant market power to dictate pricing during transactions.

The Deloitte Consumer Review (2016) found that consumers are becoming more distrustful about corporate motives and practices around the collection and use of personal data.[29] It was found that 73% of consumers would reconsider using a company if it failed to keep their data safe. By comparison, only 51% of consumers would switch companies if they were charged a higher price than competitors for a similar product.

[29] https://www2.deloitte.com/tr/en/pages/risk/articles/consumer-data-under-attack.html

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

Consumers invest in brands that they trust, and in future an increased consumer focus on trust in the cyber security of products will drive competitive advantage. We have previously considered the relationship between trust and privacy practices of consumers. In 2019, the Deloitte Privacy Index found that when downloading a mobile application, 65% of consumers cited trust in a brand as their most important consideration when deciding to grant an app permission to access personal information. This means brands must be transparent about how they will use personal information.[30] In addition, 63% of Australian consumers have consciously deleted an application as a result of their privacy concerns, and 86% of consumers reported their trust in a brand would increase after a breach if timely and transparent notification was given.[31]

The above could be similarly applied to the cyber security context, particularly where the confidentiality, integrity and availability of the product or service is affected. As data breaches and cyber incidents are becoming major headlines in the news, it is imperative for business to work towards maintaining consumer confidence in products and services. It is important for businesses not only to protect their brand from an incident, but to preserve the brand reputation even after an incident.

In future, customer experience will become the primary basis for competitive differentiation. In the competitive marketplace, it can be difficult for consumers to differentiate products and services merely on face value. Branding may serve as a competitive advantage and help businesses differentiate themselves against their competitors. This should help organisations gain business and build more meaningful engagements with their customers, which will encourage consumers to provide more willing interaction and potentially share more of their data with the business.

[30] https://www2.deloitte.com/au/en/pages/risk/articles/deloitte-australian-privacy-index.html
[31] https://www2.deloitte.com/au/en/pages/risk/articles/deloitte-australian-privacy-index.html

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

A best practice behaviour change that the Australian government could carefully consider is the uplift of cyber security in Estonia as a result of attacks in 2007 on a national basis.

The scale of attacks, leading to the term 'cyberwarfare' being applied became catalyst in developing one of the globes strongest nation's in Cyber Security. The attacks themselves catalysed actions by Government to ensuring that the aim of increasing national cyber security was met.

In order to achieve scale and encourage a national cyber culture change and uplift, transparency and media interest was encouraged, with acknowledgement of the scale of uplift required. Heavy investment from government and industry for a sustained period of time has ensured a nationwide uplift in Estonia, with increased security awareness in the public and increased security posture in government and industry.

In evaluation of the uplift in national cyber security, Estonia's current reputation in cyber security should be considered. Of note, there have been strengthened relationships with fellow European countries due to their excellence in the industry, providing point of collaboration, and a source of Cyber talent and knowledge[32].

[32] https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/

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

One feature that should be prioritised in products and services is that of cyber ratings, that are akin to safety or efficiency ratings in many other products, such as electronic appliances and motor vehicles, could be enforced to inform consumers and their choices in the market. This can help bridge the significant information asymmetry that currently exists between producers and consumers. Additions of cyber ratings to products should be a focus for solutions that will be utilising new technologies such as 5G and IoT where the average consumers may be oblivious to the technological risks and implications related to their use.

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

There is a wide variety of other areas that the Australian government should consider. These include:

- Government and corporate senior executives should be encouraged to develop their knowledge regarding cyber security, in order to understand the importance of cyber security and allow for investment in the business accordingly. Associated with this, government should consider the introduction of penalties for cyber breaches at organisations for company directors, if a breach is resulting from poor cyber security practice within that organisation
- Government should hold a central repository of cyber threat intelligence, segmented for different industries to facilitate information sharing between organisations, augmenting their capabilities – particularly for those organisations that are of smaller size, and unable to invest in advance threat intelligence capabilities
- Need for accreditation for Cyber security professionals to ensure good cyber practices are implemented in organisations
- Increased focus on cyber security at universities, including research and teaching capability development to move Australia to the cutting edge of cyber security
- Connections between State and Federal government need to be improved in order to strengthen Australia's cyber security posture in the government sphere
- Support to small and medium sized business
- Red teaming to raise awareness in organisations of cyber threats external to the organisation and identify key weaknesses in typical organisational security. Anonymized results should be shared as part of information sharing programmes so that industry may look to potential capability gaps and move to rectify these
- Incentivized education programmes for cyber security, alongside regularly reviewed current curriculum content in order to maintain learning with the pace of change of cyber security practice
- Sponsorship of students without permanent residency status by government to teach ICT/Cyber in primary and high schools for an allotted period of time (e.g. 2 years), using their skills to bridge the capability gap between teachers working in school at present and the required ICT and Cyber skills to teach good digital practice and security.