Australia 2020 Cyber Security Strategy – Call for Views

CQUniversity Response, 28 October 2019

Prepared by:

Roy Pidgeon, Chief Information Digital Officer
Peter Vanheck, Deputy Director Digital Infrastructure

Background:

CQU was invited to submit feedback to the Cyber Security Strategy 2020 Discussion Paper:
Call for views: https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-strategy-2020
Discussion paper: https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-strategy-2020-discussion-paper.pdf

Response:

#	Question	CQU Response

1	What is your view of the cyber threat environment? What threats should Government be focusing on?	• The CyberSecurity threat landscape is increasing in volume, frequency and sophistication. CQU sees this through its own experiences, relationships and sector visibility.
		• The Federal Government should focus on the following;
		  ○ Nation-state and organised crime threats
		  ○ Threats that target core utility sectors – power, water, hospitals, telecommunications, etc
		  ○ Impacts/influence of social media on significant national events – elections, census, etc
		  ○ Threats that have a direct financial impact on people
		• Government should focus on providing fit for purpose guidelines and practical advice for each sector of the economy. Legislate as a tool should only be completed through exhaustive, consultative engagement with in-built protection to ensure the legislation is measured against the outcomes.

2	Do you agree with our understanding of who is responsible for managing cyber risks in the economy?	• CQU agrees with the ecosystem identification and acknowledges there are shared responsibilities and risk across these organisations. • Government should focus on removing the impact of silos across the ecosystem including engaging with industry bodies representing these organisations.
3	Do you think the way these responsibilities are currently allocated is right? What changes should we consider?	• Every Australian is responsible and should be a part of the overall Cybersecurity solution. Government, Industry and community all have a crucial roles to play in developing and improving Australia's overall Cybersecurity maturity. • Changing one sector's role, responsibilities or accountabilities is not the best way forward. Developing these for all three sectors will produce a balanced and better overall result. • The JCSC is a strong step towards creating greater unity between sectors and groups.
4	What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?	Governments should, • Establish and classify critical services (including non-Government) to Australia and develop through partnerships appropriate defence and incident response plans to support these organisations and communities to deter and manage CyberSecurity threats and events. • Partner with Telcos to prevent and respond to incoming threats to Australia • Partner with other trusted countries to deter and prevent nation-state inclusion and influence in Australian affairs. Using that collation to influence to promote and enforce good cyber-behaviour. • Partner with other trusted countries to deter, prevent and dismantle cyber-criminal organisations • Develop and promote guidelines including promoting awareness (similar to other significant health and safety campaigns)
5	How can Government maintain trust from the Australian community when using its cyber security capabilities?	The Government can gain trust from Australian communities by: • Partnering with cybersecurity industry experts to understand the real challenges, technically what is possible, what should and shouldn't be done • Accept advice and recommendations from these sector experts • Continue to improve protection of Government networks and systems, after all that's is where some of Australians most important personal information resides.

		• Building trust through greater transparency between levels of government and security agencies
6	What customer protections should apply to the security of cyber goods and services?	• Improve our Australian Privacy regulations so that they align with international best practice • Add supply chain inclusion amendments within existing legislation to protect data owners (organisations and customers) from poor supplier and third party practices • Update legislation to meet the changing online digital environment that Australians live and conduct business in
7	What role can Government and industry play in supporting the cyber security of consumers?	• Consider promoting standards that enable promotion and services/products badged as “CyberSecure” with rating levels. • Create an environment of “no blame” for victims of cyber attacks to encourage reporting, and promote support and recovery services
8	How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?	To increase the security, quality and effectiveness of CyberSecurity and digital offerings Government need to encourage solution development that consider user experience to ensure adoption. Regularly engage with the relevant cybersecurity, industry and community experts to ensure design and adoption is appropriate and effective.
9	Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?	• Protecting Government networks, legislation development and enforcement and awareness should remain with the government. (Not devolved to the private sector), to avoid introducing commercial bias. The risk of Nation State influence over private sector organisations is too great. • Consider developing a low cost cybersecurity advisory, SOCaaS and response services for small business or at risk organisations could be Government sponsored and devolved to the private sector
10	Is the regulatory environment for cyber security appropriate? Why or why not?	Regulatory environment for Cybersecurity is incomplete. Australia should have specific cyber legislation instead of relying on amendments to old and pre-digital legislation that does not clarify roles across levels of government. The effect of this additional complication through many amendments is that it can be difficult to understand, implement and leave gaps in responsibilities and enforcement.

11	What specific market incentives or regulatory changes should Government consider?	• Market incentives – engage with expert members of industry and community who are well known for cyber and digital innovation. Resist over-regulating cyber/digital.
		• Consider supporting Cybersecurity industry and companies raising maturity through:
		  ○ Tax incentives/rebate for innovation in cybersecurity
		  ○ Incentives for investment in cybersecurity
		  ○ Rebates for SME's and smaller institutions who will struggle with costs of cybersecurity investment

12	What needs to be done so that cyber security is 'built in' to digital goods and services?	Develop and promote the idea of 'built in' cybersecurity; Government responsibilities should include; • Set up standards and badge / promote effectively (eg. Government approved "CyberSecure Site") • Develop rigorous certification processes • Operate a testing and validations service. Develop verifying technologies to support testing – make these available to the community Industry responsibilities should include • Development of strong and reliable systems • Improving cybersecurity practices/processes for their goods and services • Supporting third party software/hardware testing and validation processes and tools
13	How could we approach instilling better trust in ICT supply chains?	Setting up and operating a certification system (see Q12) will enable a sector wide approach and result in development of higher quality supply chains. This will create transparency without exposing IP or intricacies of configuration unnecessarily. Cybersecuity awareness campaigns need to be broad ranging and extend well beyond the once per year CyberSecurity week campaign.
14	How can Australian governments and private entities build a market of high quality cyber security professionals in Australia?	High quality cyber security professionals do not come from education and training alone. Mixing good quality training with actual o-the-job experience makes for high quality cyber security professionals – this takes time and a commitment from Government, Industry and community. • Training – should be delivered by experts and not any organisation that sees a business opportunity

		• Work experience through relevant placements underpinned by Government supported training incentives
		  • Training organisations should be responsible to delivery work experience through placement
		  • Organisations should be encouraged to take cyber security trainee's and provide work experience

15	Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?	Yes, cyber-insurance is generally very immature and under-developed with limited providers (with a real understanding of what it required) participating in the market. They typically offer boxed cyber-insurance packages or designer packages. Both of these feel a bit like 'best guess' offerings. Insurance companies are in the risk (and profit) business – cyber risk is relatively new and misunderstood. Time, demand and claims will help to mature this market.
16	How can high-volume, low-sophistication malicious activity targeting Australia be reduced?	• Awareness, alerting and training. All Australians have a shared responsibility to manage and limit this type of cyber threats. Government should lead general public education campaigns. • Embed appropriate cyber awareness into K-12 curriculum. Support life-long-learning in Cyberskills development and re-skilling workforces to assist with cyberskills demand. • Encourage targeted activity by Telco sector supported by Government intelligence to block malicious activity at geographic boarder.
17	What changes can Government make to create a hostile environment for malicious cyber actors?	• Appropriate legislation to support the prosecution of cyber-criminals • Actively pursue (offensively) through cybersecurity means under existing enforcement services or creation a new enforcement service
18	How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?	No comment
19	What private networks should be considered critical systems that need stronger cyber defences?	No comment
20	What funding models should Government explore for any additional protections provided to the community?	The increasing threat levels and risk demand investment in education, awareness and supporting frameworks and systems. It is difficult to see how this can be apportioned back to community or industry groups directly.

21	What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?	• There is no single information sharing platform or cyber community collaboration that the sector uses • Alerts, notifications and IOCs are sourced from a variety of sources – it can be easy to miss important contextual warnings
22	To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?	This is true and likely a little over-generalised, awareness will be different across sectors and seems linked to investment of CyberSecurity awareness and training. • Enterprise and large organisations – higher degree of awareness • Mid-size organisation – some awareness • Small business and regular people – very low.
23	How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?	AU businesses will be required to improve the cybersecurity of their good and services; as consumers become more aware, they will demand better support/integration of cybersecurity in the products or services they buy or they will take their purchasing power elsewhere.
24	What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?	CQUniversity runs a Cyber Awareness campaign based on CyberHero action comic book style characters; they are based on real ICT people with not so secret identities handing out real Cybersecurity tips and tricks. It has been very successful at the University in raising awareness and engagement on otherwise technical and dry topics. The University tracks and measures several indicators that indicate improved awareness of main threats people are exposed to online. Interactive online training courses for induction and annual security, data handling and privacy awareness are also built around this “themed” awareness campaign.
25	Would you like to see cyber security features prioritised in products and services?	Yes, it is a sign of quality goods or service. There are some goods and services that do display cybersecurity credentials as a part of their brand and marketing. This should be encouraged and supported by a government backed standards and badging regime that is part of an overall awareness and education campaign.
26	Is there anything else that Government should consider in developing Australia’s 2020 Cyber Security Strategy?	n/a