Southern Cross University

Technology Services

Australia's 2020 Cyber Security Strategy – Call for Views

Southern Cross University's response

Q #	Question	SCU Response
1	What is your view of the cyber threat environment? What threats should Government be focusing on?	The cyber threat environment is comprised of, often common, threats to public and private organisations and individuals. These threats include nation states as well as relatively unsophisticated threat actors. Due to the increasing technical interconnectedness of society, security is 'a team activity'. Given the negative externalities from poor cyber security of those connected, Government needs to coordinate and lead. However, the initial focus should be on providing fit for purpose guidelines and practical advice. A particular challenge is the penetration of artificial intelligence and IoT technologies. Potentially these could increase the capability of both cyber protection and threats.
2	Do you agree with our understanding of who is responsible for managing cyber risks in the economy?	Yes, we agree. However, more attention needs to be paid to the interactions between each of these groups. Also, consideration for consumers to better assist them in understanding the cyber security threats to better prepare and respond to them. Government run programs, such as a cyber security rating system for cyber security goods and services, might provide improved awareness for consumers.
3	Do you think the way these responsibilities are currently allocated is right? What changes should we consider?	The current allocation of responsibilities should reflect the connections and interaction between sectors and groups. The Government agencies should provide proactive approaches to address the disparity between smaller organisations and cyber threat actors allowing for improved scale and efficiency. Consider JCSC proactively engaging with the various groups within their responsibility. Additionally, they might act as an initial point of contact for cybersecurity expertise.
4	What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?	Increase proactive focus on cybersecurity as a risk on equal footing with other national, organisational and individual risk. Consider providing cyber threat intelligence feeds to institutions and business as well as leading Australia's cyber threat intelligence strategy domestically. Implement an effective awareness campaign to ensure cybersecurity is front of mind for consumers. This should be done through constant promotion, multifaceted strategies in the media similarly to other national campaigns (drink driving, sun safety, healthy heart).

		The Government should engage in diplomatic discussions to bring influence to address the threats, that institutions and businesses have no capacity to affect. These channels can reduce the likelihood of attacks from nation states, or potentially encourage the awareness that Australia is proactive and will not be an easy target.
5	How can Government maintain trust from the Australian community when using its cyber security capabilities?	The Government should consider being transparent around the use of its cyber security capabilities to maintain and build trust with the Australian community. This information might include general capability and the guidelines for when and how this capability will be used. This needn't include any information about specific capability, procedures or targets. Raising community awareness of cybersecurity and providing leadership will also support transparency and increase trust within the community. Consider improving the consistency of legislation between jurisdictions. Cybersecurity is a national concern needs to have a consistent, effective national approach.
6	What customer protections should apply to the security of cyber goods and services?	Implement a readily recognisable rating system for cyber security related goods and services. This will identify organisations and services that are cyber leaders while also provide consumer awareness of the capability of the goods and services in relation to cyber. This should include strong alignment with existing privacy, data governance and ownership legislation and guidelines.
7	What role can Government and industry play in supporting the cyber security of consumers?	Implement a readily recognisable rating system for cyber security related goods and services. This will identify organisations and services that are cyber leaders while also provide consumer awareness of the capability of the goods and services in relation to cyber. An effective awareness campaign is required to ensure cyber security is front of mind for consumers. The Government should lead the national conversation through constant promotion, multifaceted strategies in the media, raising awareness similar to other national campaigns (drink driving, sun safety, healthy heart). Improve the transparency of Cyber security related law and repercussions of infringement, including the education of victims with regard to reporting and available support. This should encourage a no blame point-of-view for victims of cyber-attacks to encourage reporting. Where possible, the publication of lessons learnt after breach notifications. These should reinforce a no blame point-of-view for victims. These publications could provide opportunities to share,

		without recrimination, and allow organisations to act on the lessons learnt and proactively address the risks within their organisations.
8	How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?	Implement a readily recognisable rating system for cyber security related goods and services. This will identify organisations and services that are cyber leaders while also raising awareness within the community and may provide competitive advantages to organisations that participate in the system. Such a system can also raise the effectiveness of cyber security products and services through the standardisation of offerings and provide consumer awareness of the capability of the goods and services in relation to cyber. Consider the publication of lessons learnt after breach notifications where possible; particularly within the same vertical sector. This will provide opportunities to share leanings without recrimination and allow organisations take actions which might reduce the impact to them. Where this occurs, organisations which have shared should be acknowledged.
9	Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?	Consider the privatisation in regional services where the market is not able to provide their cost-effective delivery. However, a risk-based approach reviewing environment and threat is required to ensure cybersecurity accountability is addressed in any privatisation.
10	Is the regulatory environment for cyber security appropriate? Why or why not?	The regulatory environment for cyber security is not appropriate at present. This is due to dated and incomplete legislation with variation across regions, states, and industry sector verticals which is not capable of addressing the current and future cyber threats.
11	What specific market incentives or regulatory changes should Government consider?	Tax incentives for early adopters and achieving levels of certification could be provided through tax incentives. Consider the increase of funding to cyber security related agencies and support to industry groups. Additionally, broaden the scope of eligibility and increase the funding and support of post start-up and commercialisation of innovation.
12	What needs to be done so that cyber security is 'built in' to digital goods and services?	An easy to interpret rating system for consumers to judge the cyber security of products and services. A broad and ongoing awareness campaign to increase consumer demand for better cyber security. Incentivising Australian business participating in the supply of cyber security related products and services should also be considered.
13	How could we approach instilling better trust in ICT supply chains?	Consider implementing a rating system for cyber security related supply chains. This rating should be readily recognisable for goods and services that establishes a base level of cyber protection. This will identify organisations and services that are cyber leaders while also raising awareness within the community and may provide

		competitive advantages to organisations that participate in the rating system. Such a cyber security rating system should be widely promoted with consumers. Additionally, a rating system would help domestic markets compete potentially less secure, imported products. Incentivising Australian business participating in the supply of cyber security related products and services should also be considered.
14	How can Australian governments and private entities build a market of high-quality cyber security professionals in Australia?	Consider a strategy of lifelong learning. This might commence during school, be embedded in graduate qualifications, and incentivised through ongoing professional development. Supporting parents through training on the digital footprint and security hygiene should be considered. Additionally, consider better informing the older demographics, on how best respond to common attack vectors. Given this investment, an increase in human capital flight pull factors should be considered. This may include the promotion of Australia's education, innovation, democracy, human rights and liberal values. Similar to how skill shortages in remote areas are addressed, consider exploring opportunities to ensure the cyber skill base has an opportunity to stay in Australia and support regional communities.
15	Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?	Lack of clarity regarding the expectations of cyber insurance industry. This lack leads to poorer understanding of the benefits and shortcomings surrounding cyber insurance market. This might be addressed through provision of standards and guidelines detailing in both in legal and plain English what is covered, terms, timing, service levels and outcomes from enacting cyber insurance. Also, information such as what controls might reduce the cost of cyber insurance, how the effectiveness of these controls can be demonstrated, what information is required to make claims, and the likelihood of the payment of claims could be clearer to prospective insures. Minimum policy information requirements may be helpful along with the standardisation of what policies cover.
16	How can high-volume, low-sophistication malicious activity targeting Australia be reduced?	With the support of Government and intelligence agencies, encourage the Telecommunication sector to block malicious traffic entering and within their networks where economies of scale can be realised. This may benefit from guidelines to provide the minimum standards of this protection.
17	What changes can Government make to create a hostile environment for	Enhancing the offensive cyber capabilities of the Australian government along with other punitive measures should be considered. These measures might include more streamlined extradition agreements for cyber related crimes. The community

	malicious cyber actors?	should also be made aware of these capabilities and measures, potentially by promoting and encouraging media reporting on successful prosecutions. Consider steps to increase the resilience of previous 'soft targets' in the community, such as older citizens who may not have the digital literacy that other generations possess. Along with a national coordinated and concerted effort to raise the cybersecurity posture, may result in Australia being categorised by malicious cyber actors as a high cost, lower value target.
18	How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?	No response.
19	What private networks should be considered critical systems that need stronger cyber defences?	No response.
20	What funding models should Government explore for any additional protections provided to the community?	Increased funding is required to address the rising volume and sophistication to cybersecurity attacks. Allocation of this funding should risk based and utilise a framework, to assist in reviewing the risk and communicating the expected outcomes. Effective awareness campaign could particularly benefit from increased funding. Similar to other national campaigns (drink driving, sun safety, healthy heart), the Government can lead the cyber security conversation through constant promotion beyond an annual Cyber Awareness week. Broadly imbedding cyber security in education and training could produce a more cyber aware workforce. The focus should be on lifelong learning, commencing through school, embedded in graduate qualifications and incentivised through ongoing professional development ensuring future generations have digital and cyber literacy in their DNA. Given this investment, an increase in human capital flight pull factors should be considered. This may include the promotion of Australia's education, innovation, democracy, human rights and liberal values.
21	What are the constraints to	Outside the technical, intelligence and government communities, the community is largely unaware of the cyber security related work that

	information sharing between Government and industry on cyber threats and vulnerabilities?	the government carries out. The option to provide an 'opt out' information and advice channel would help address this. However, the channel should provide a clear understanding of the benefits of the communication to the recipient, to ensure the community is engaged in the content.
22	To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?	Strongly agree that the lack of cyber awareness results in poor consumer choices, but equally there is limited information available in the supply chain to make an informed decision. Criminals using more sophisticated social engineering in their cyber-attacks, and the lack of awareness makes informed decisions challenging.
23	How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?	The Government should take a leadership approach on awareness. Media is currently leading community awareness, often resulting a public concern rather enabling improved choices. Government could provide an informative and empowering message to the individuals who may feel the most concerned.
24	What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?	There are a number of examples of successful campaigns that have caused consumers to change their behaviours. Examples of this sort of campaign include such as SunSmart, quit smoking and tourism. Also, campaign should have a simple message and focus on the use of digital channels to best reach its intended audience. For example, social media and digital streaming platforms. Further targeting of less cyber aware demographics might also be considered.
25	Would you like to see cyber security features prioritised in products and services?	Strongly agree that cyber security features be prioritised in products and services. However, any related guidance should be simple to allow consumers to make use of it. Consider a focus on newer technologies with broad impact, like IoT, where the market and industry are still maturing.
26	Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?	Clearly stating the strategic goals and how they will be measured would assist in interpreting and implementing the Strategy. Also, analysis should be undertaken of similar strategies from other countries to determine what has and hasn't been successful to date.