Charles Sturt University

DEPARTMENT OF HOME AFFAIRS

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

1 November 2019

Office of the Vice-Chancellor
Charles Sturt University

Charles Sturt University

Office of the Vice-Chancellor

1 November 2019

The Hon Peter Dutton MP
Minister for Home Affairs
Parliament House
CANBERRA ACT 2600

Dear Minister

AUSTRALIA'S 2020 CYBER SECURITY STRATEGY – A CALL FOR VIEWS

On behalf of Charles Sturt University, I am pleased to provide you with this submission in response to your call for views on Australia's 2020 Cyber Security Strategy.

Charles Sturt University is Australia's largest regional university, with more than 43,000 students and approximately 2,000 full time equivalent staff. We are a unique multi-campus institution with campuses at Albury-Wodonga, Bathurst, Canberra, Dubbo, Goulburn, Manly, Orange, Parramatta, Port Macquarie and Wagga Wagga, as well as various study centres located throughout regional and rural south-eastern Australia.

Charles Sturt University has deep and proven experience in safety, security, justice and emergency services, including cyber security.

Charles Sturt University welcomes the Australian Government's commitment to the ongoing development and implementation our nations next Cyber Security Strategy as part of its commitment to protecting Australians from cyber threats. The University notes that the new strategy will be a successor to Australia's landmark 2016 Cyber Security Strategy, which set out the Government's four-year plan to advance and protect our interests online. It is appropriate that the new strategy builds on the Government's investment to position Australia to meet the rapidly evolving cyber threat environment.

Charles Sturt University appreciates the opportunity to contribute to the development and implementation of the Cyber Security Strategy as part of consultation process to shape the new strategy's development. The University's submission provides a range of views on the steps the Government can take to improve the cyber security of Australian citizens, community groups and businesses, including Australia's universities.

Charles Sturt University has prepared this submission in accordance with the structure and content of the *Australia's 2020 Cyber Security Strategy – A Call for Views* (refer, Australia's 2020 Cyber Security Strategy - discussion paper (2MB PDF)) and provided for reference at Attachment A.

Threat environment

The rapid advance of technology, particularly the information technology that powers the modern digital world, brings enormous benefit to the economy, society and the environment. However, the 21st Century's reliance on information technology exposes society to new threats from those who wish to do us harm, be they state-actors, competitor organisations, individual and organised crime or terrorist groups. As discussed in the Strategy, the rapid pace of change in cyberspace and the extent of the modern world's reliance on the internet means governments, businesses and individuals cannot be complacent.

Charles Sturt University agrees that the loss of an essential service like electricity, water or transport has the potential to cripple the economy, causing social unrest and, ultimately, damage our welfare and way of life. Recent incidents such as compromises of the Australian parliamentary networks, universities and key corporate entities, illustrate the scale of the threat. Not only do such attacks damage specific organisations, they provide mechanisms for those who seek to undermine Australia's democratic values and liberal institutions.

The cyber security threat facing Australians, our businesses and organisations, as well as government is real and ever-growing in terms of the breadth and sophistication of threat. No more so than the defence and military threat posed by failures in cyber security as well as the concomitant threat of foreign interference. Strategies for preventing and responding to defence, military and foreign interference cyber security threats are the realm of the Australian Government.

Charles Sturt University agrees with the analysis provided in the Strategy, that serious cyber incidents like WannaCry, Cloud Hopper and the intrusion into Australia's parliamentary networks illustrate the threat to our economy, democracy and way of life. Further, the University agrees that to protect nationally significant systems Australia must position itself as a world leader in cyber threat detection, prevention and response. To meet this challenge governments, businesses and our education and training institutions will need to work more closely together than ever before.

As stated in the Strategy, cyber security incidents have been estimated to cost Australian businesses up to $29 billion per year and cybercrime affected almost one in three Australian adults in 2018. For businesses, a more secure cyberspace will support the delivery of digital services that Australians have come to expect. There is no question that cyber security will underpin Australia's future economic growth, however, strategies for ensuring cyber security must be customised and tailored to ensure Australian businesses remain competitive through creativity and innovation.

Charles Sturt University supports the elements of the Strategy that focus on individuals and families. In the short to medium term much more support and assistance will be needed to keep individuals and families safe online. The long term the building of community-wide and individual cyber skills and knowledge, however, will provide the only practical solutions to keeping individuals and families cyber safe. The tertiary education and training sector have a vital role to play in the development of long-term individual and community cyber resilience. The University agrees that every Australian should have the confidence that they can keep themselves and their family safe while taking advantage of the online world. Developing such resilience will also be essential in achieving the Government's Digital Transformation Strategy goals.

Finally, Charles Sturt University is of the view that the accountabilities and responsibilities of government, business and the community in Australia's cyber security as set out and currently implemented in the *Australia's Cyber Security Strategy* (refer, https://cybersecuritystrategy.homeaffairs.gov.au) are both effective and efficient. The University does however stress, that as the external cyber environment is constantly changing, Australia's cyber security arrangements will need to be constantly monitored, risk assessed and continually improved. Quality assurance of the development and implementation of Australia's future cyber security strategies and the communication of the rationale for the strategies and what they mean for government, business and the community will be essential to ensure success.

Role of governments in a changing world

As a result of the technology drivers, Australia's critical systems, including in the energy, telecommunications and transport sectors, are becoming increasingly digitised. While technology has driven significant productivity gains across the economy in recent decades, it has also exposed society to increased cyber threat, as discussed above. As mentioned in the Strategy, international cyber incidents have disrupted power grids, degraded public health and transport systems, and damaged physical infrastructure. If realised in Australia, such threats have the potential to impact physical safety, economic security and the continuity of government and its services.

With the emergence of the Internet of Things (IOT) and interactive electrical devices, from smart phones, to television to refrigerators and home security and energy systems, Australians are relying on the internet and digital services more than ever. Technologies such as automation, artificial intelligence and virtual reality will continue to transform the way we live, work and interact with each other as the IOT increasingly reaches into every aspect in modern life. As discussed in the Strategy, these changes bring unprecedented opportunities for all Australians, however, they also make us more reliant on technology and potentially more vulnerable to malicious cyber activity.

While there is a leadership and a whole-of-nation role for the Government in cyber security strategy, all parts of society have a role to play, from the individual, to the family, local community and government, NGOs and business from small to large and finally industry more broadly and multinationals. Any strategy involving all partners must define roles, responsibilities and accountabilities for action which, given the complexity of the cyber security space, will most likely require a matrix approach which brings together threat risk and response capability of each actor.

As discussed in the section above, without overly simplifying the digital world, information technology provides new ways of doing things rather than creates new things to do. To this end, legislative frameworks for cyber security should build on and be integrated with existing regulatory arrangements. For example, Charles Sturt University notes that the Strategy mentions the business to business gap in consumer law. While a new and emerging discipline, it is highly likely that the expansion of consumer law to business to business cyber interactions will be required, particularly to protect the interests of micro, small and medium firms. This need is likely to be even more necessary in regional, rural and remote Australia, where cyber workforce skills and knowledge can be lacking.

This is an example of amending existing legislation and regulation to take into account cyber security, rather than creating a whole new suite of stand-alone legislative frameworks and regulatory arrangements. By taking this approach to legislation and regulation it will be easier for governments to communicate the importance of cyber security and for businesses and individuals to comprehend and understand the impact of cyber security considerations.

Finally, Charles Sturt University agrees that cyber security requirements for providers of essential services are a potential weakness in our ability to respond to crisis, for example the failure of emergency services communications during fire or cyclone. The University acknowledges that there is already mature cyber security arrangements in place for some services. There are, however, minimal or highly variable requirements with different standards of enforcement, particularly where services are provided across different levels of government or by many smaller organisations (like water and sewerage services). The University agrees that the best approach to this challenge would be consistent but flexible cyber security laws for critical systems. Further, the University suggests that such arrangements be governed nationally through a COAG Ministerial Council.

Australia's future cyber security strategies and the communication of the rationale for the strategies and what they mean for government, business and the community will be essential to ensure success. Effective communication on this front by Government will be essential to ensure the Australian community maintains trust in the national cyber security capability. Maintaining trust in the national cyber security capability will be crucial to underwrite the confidence of the Australian people in governments, businesses and community organisations through the 21st Century.

Enterprise, innovation and cyber security

As discussed in the sections above and addressed in the Strategy, the technology sector is the cornerstone of Australia's growing digital society and digital economy. As the IOT increasingly impacts on our daily lives, information technology will increasingly play the key enabling role in the design, manufacture, delivery and management of consumer online experiences.

The Strategy is correct to identify that businesses drive Australia's digital economy, which is essential to our prosperity and that if something involves the internet, it will involve an innovative business. However there is always, and perhaps increasingly so, going to be a trade-off between cyber security and creativity, innovation and enterprise. To this end, Charles Sturt University agrees with and supports the following element of the Strategy.

> *"Government plays a role in facilitating private sector success, be they individuals, small to medium or large businesses. Clear and reasonable rules that protect consumers and keep risky businesses out of the market are good for everybody. But there is always a balance Government must strike – obligations that are unclear or onerous can discourage innovation and reduce our international competitiveness. On the other hand, the rules that protect and support Australians should keep pace with the extreme rate of technological change in rapidly evolving sectors of the economy. The variability in the security of cyber goods and services raises the question of whether it is reasonable to expect providers to do more to protect their customers. Adding to this is the question of whether a purchaser is adequately equipped to protect themselves."*
>
> From – Page 11, *Australia's 2020 Cyber Security Strategy – A Call for Views.*

While in the short term, say through to early next decade, the Government may need to include direct actions in its Strategy to ensure consumers can be confident products and services include reasonable cyber security protections, in the longer term such an approach will not be sustainable. In the long term, as the IOT becomes our way of life, a combination of consumer law strengthened for the digital world and individual cyber skills and knowledge, through education and training from early childhood to tertiary will be required to ensure cyber safety. Identifying gaps in this space will need to be ongoing and will require input from all sectors of society.

Trusted marketplace with skills professionals

Society's trust in the technology marketplace, together with the skills and knowledge of technology professionals will be crucial to ensure cyber security. This theme builds on the commentary provided above regarding communication and awareness and understanding through education and training.

Charles Sturt University agrees with and supports the following elements of the Strategy that address the technology marketplace and the skills and knowledge of technology professionals.

> *"Increased reliance on technology underscores the need for higher standards of cyber security to maintain the availability and integrity of critical services. This trend means demand for secure products and services as well as skilled cyber professionals will continue to increase. However, it is difficult for many businesses and consumers to understand what level of security is embedded in digital products or what level of service a professional can provide. Cyber security decisions made by businesses and consumers, when added up together, can have implications for Australia's economy and national security."*
>
> And.
>
> *"A trusted market of secure technologies, products, services and professionals is critical for improving cyber security outcomes in Australia. By 'trusted market' we mean an open, transparent, diverse and competitive technology market, where vendors include cyber security protections as standard and buyers clearly understand any risks. Ideally, digital products and services should have security built in 'by-design', so that users do not need to have any expert knowledge. Similarly, businesses of all sizes need to be able to trust their suppliers and get access to expert advice when needed. Globally it appears that the mechanisms and incentives for this to occur, such as visible and trusted industry standards, do not yet exist in most cases."*

And.

> *"Access to skilled professionals is an important part of a 'trusted market'. Government continues to receive feedback about a cyber security skills gap in Australia. AustCyber estimates that there were 2,300 fewer skilled cyber security professionals than required in Australia in 2018. Up to an additional 17,600 will be needed by 2026. Some stakeholders also have raised concerns about whether the education and training system is meeting the needs of the cyber security sector, and whether sufficient data is available on this issue. Part of the problem could be confusion about what qualifications are needed for what cyber security jobs – awareness, information, skills and knowledge."*
>
> From – Page 13, *Australia's 2020 Cyber Security Strategy – A Call for Views.*

Strategies and actions to be included in the *Australia's 2020 Cyber Security Strategy* will need to contemplate and take into account these technology marketplace and professional skills considerations. Charles Sturt University agrees that developing strategies and implementing actions to address these issues will need to answer:

> *What could be done to ensure that a minimum standard of cyber safety is provided in digital goods and services, simultaneously ensuring that our civil liberties aren't compromised, so as to protect community and business?*
>
> *How could we approach instilling better trust in ICT supply chains?*
>
> *How can Australian governments and private entities build a market of high-quality cyber security professionals in Australia?"*
>
> From – Page 14, *Australia's 2020 Cyber Security Strategy – A Call for Views.*

Building on the University's COAG Ministerial Council suggestion above, Charles Sturt University recommends that a Ministerial Council for Cyber Security be convened and chaired by you to address the technology market and professional skills on an ongoing basis. Such a Council would include members drawn from industry, academia and the community.

Finally, Charles Sturt University agrees that cyber insurance provides a last line of defence in technology markets and workforce. It is an essential element to maintain a trusted market, particularly in business to business transactions. To our knowledge many insurance options exist for policy holders to prevent, respond and recover from cyber incidents. Further, the University agrees with the observation that there is a relatively low take-up of cyber related insurance products amongst Australian businesses. Interestingly, communication with a number of our service providers suggests that lack of knowledge is the greatest barrier to uptake, rather than the cost of policies themselves.

Hostile environment for malicious cyber actors

Charles Sturt University agrees with and supports the following elements of the Strategy that address the hostile environment in which malicious cyber actors operate.

> *"Given the scale and reach of the threats across the economy, we currently place a heavy emphasis on tending to victims through incident response. This can come at the expense of stopping threats from getting to the victim in the first place. We won't be able to arrest our way out of this situation, so increased law enforcement capability and capacity will help, but not solve the problem."*

And.

"The current approach relies on a victim's own decision-making skills to prevent the kind of damage that happened from campaigns such as WannaCry. This type of ransomware is just one example of a threat that could be countered on a much larger scale if preventative measures are put in place. Such measures would aim to make Australian networks harder to exploit, although we can never be totally cyber secure."

From – Page 14, *Australia's 2020 Cyber Security Strategy – A Call for Views.*

Consistent with commentary provided above, Charles Sturt University believes that Australia's approach to cyber security must transition from incident response (after the event) to stopping threat (before the event). The *Australia's 2020 Cyber Security Strategy* provides an excellent opportunity to commence this transition in approach to cyber security. Ideally by mid next decade this transition would be achieved.

Further, Charles Sturt University agrees that:

"Between those two ends of the spectrum lie a range of actions – mid-level capabilities. Such measures can include gathering information on actors targeting Australia, sharing advice on hostile activity between entities involved in defending networks or blocking known malicious actors. Australia already works closely with international partners to share information and build support for international rules and norms to govern the responsible use of cyber space."

From – Page 14, *Australia's 2020 Cyber Security Strategy – A Call for Views.*

And.

"The Government will always play its part in countering the most sophisticated and dangerous threats to the nation, but it is becoming increasingly important for this to be supported through partnerships and collaboration with industry. The number of critical privately owned or operated systems at high risk of malicious activity is growing and therefore the number of close partnerships between Government and industry may need to grow."

From – Page 15, *Australia's 2020 Cyber Security Strategy – A Call for Views.*

Again, as set out in the Strategy, Charles Sturt University agrees that developing strategies and implementing actions to address these issues will need to address a range of issues, including.

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

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

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

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

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

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

From – Page 16, *Australia's 2020 Cyber Security Strategy – A Call for Views.*

And, again, Charles Sturt University recommends that a Ministerial Council for Cyber Security be convened and chaired by you to address these issues on an ongoing basis.

Cyber aware community

As discussed in several sections above, Charles Sturt University is of the view that ultimately the long-term response to cyber security threat lies in creating a cyber aware community. To this end, the University supports and agrees with the following elements of the Strategy.

> *"Australians need the right knowledge to make cyber-smart consumer choices. We need to know when to demand better cyber security features from the products and services we use. And we need to know how to be more consistent in practicing secure online behaviours. Human behaviour is the most significant weakness exploited in cybercrime. Successful attacks often rely on an end-user's lack of cyber security understanding, using methods such as mass phishing email campaigns as well as the more targeted attacks such as spearphishing or whaling. The FBI's Internet Crime Complaint Center's 2018 Crime Report revealed they received just over 20,000 reports of Business Email Compromise attacks with adjusted losses of over US$1.2 billion that year alone."*
>
> And
>
> *"We aren't born with knowledge of cyber security. It is through education that risks are appreciated and the measures to mitigate them are learned. But like all other forms of security, awareness is a complement to, not replacement for, the availability of secure features. For example, drivers are provided with a seat belt in addition to education about the importance of road safety and incentives to use the seat belt. And the same expectations and requirements we have where safety is paramount should apply in cyberspace.*
>
> *The question then becomes how to empower consumers to demand services and products that have been designed with cyber security in mind. We will need to leverage community and industry partnerships to gather the evidence about what behaviour change initiatives work best and roll them out at scale. Secure online behaviours should be as common as locking the door at home. But user-awareness across both private and business environments is generally still too low."*
>
> From – Page 16, *Australia's 2020 Cyber Security Strategy – A Call for Views.*

Technology and market education and training from early childhood to tertiary education and training will be essential to ensure the development of a cyber aware community. This will not only take time, but will require substantial investment in knowledge creation and skills development. This investment will need to be forthcoming from government for formal qualifications and business for workplace skills, together with investment by individuals in their own professional (and personal) development.

Education and training investment to ensure that all members of the Australian community are equipped with the relevant technology skills to both work in the cyber world and to protect themselves as individuals and families, will ensure that:

- A high level of cyber awareness will drive good consumer choices and in turn, the provision of safe market offerings.
- Increased consumer focus on cyber security will enable Australian businesses to develop, make and sell, secure safe cyber products, with the consumer accepting an element of the cost of safety in product price.
- Consumers demand cyber security features in products and services.

Again, development of specific actions in this space and the investments and programs to deliver them should be informed by the work of the Minister's Cyber Security Council that we propose, above.

Further, drawing on the success of community awareness programs such as smoking, road safety and drink driving, the development of a long-term approach to community awareness of cyber security will need to complement education and training investments. While the Strategy touches on this element, the Strategy (and funding for it) could be significantly strengthened on this front. The development and implementation of a long-term cyber security community awareness program would not only provide an immediate, positive impact but would also be an initiative the Government could develop and implement immediately.

In conclusion, Charles Sturt University believes that for the Strategy to be successful, it will need to be developed and implemented in partnership with the Australian community. The University agrees that by working together, governments, academia, industry and the community can strengthen Australia's cyber resilience across the economy to ensure we prosper as a nation and protect our interests online. Our recommendations relating to a cyber COAG Ministerial Council chaired by you on the technology marketplace and professional skills would provide a mechanism to effect this requirement for success.

I would be very pleased to provide further information for your and the Department's consideration and would be available to provide evidence at any proposed consultations that the Department may undertake in relation to improving the cyber security of Australian citizens, community groups and businesses, including Australia's universities.

Yours sincerely

Professor Heather Cavanagh
Acting Vice-Chancellor