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

Department of Home Affairs

8 November 2019

Executive Summary

The University of Melbourne welcomes the opportunity to respond to the call for views on Australia's 2020 Cyber Security Strategy.

The development of a new Cyber Security Strategy represents a key opportunity to re-align Australia's cyber security framework to emerging threats and challenges. The University of Melbourne appreciates the consultative approach the Government is taking. Allowing stakeholders a chance to provide input will help to ensure that the Strategy represents a holistic outlook on cyber security, leading to a more robust framework. We are also pleased that the Strategy Paper identifies a number of the key components of a successful cyber security strategy, including a vibrant research innovation system and a skills framework that is aligned to the needs of the cyber industry. We also welcome the recognition of the importance of integrated consideration of new issues arising in the protection of cyber-physical systems.

We argue, however, that the Strategy Paper has shortcomings in several areas. To a large extent, these shortcomings concern the questions that the Strategy paper does not raise rather than those that it does. While the Paper addresses the importance of public trust, it fails to adequately emphasise the need for safeguards around individual autonomy and privacy in order to build and maintain this trust. Government interventions that are intended to bolster cyber security but that are perceived to erode privacy or autonomy will undermine public confidence in the cyber security agenda. The 2020 Strategy should be explicit on the need to balance security measures with appropriate safeguards, including appropriate limits on the Government's powers to intervene on individual devices.

The comments below also raise a number of further points that we argue should be reflected in the 2020 Strategy. These include:

- A commitment to an open funding framework for cyber research, possibly modelled on the funding mechanisms of the Defense Advanced Research Projects Agency (DARPA) in the United States;
- A commitment to increasing the number of cyber skilled professionals in Australia, significantly beyond the additional 17,600 the Strategy Paper concludes will be needed by 2026;
- Increasing the requirements around responsible disclosure of vulnerabilities for both Government agencies and businesses;
- A shift in focus from cyber awareness to cyber behaviour; and
- Greater visibility of the imperative to align with developments in the international arena.

We would welcome the opportunity to discuss these matters and other issues related to the development the 2020 Cyber Security Strategy.

For further information or to discuss this submission please contact Professor Liz Sonenberg, Pro Vice-Chancellor (Digital and Data)) at l.sonenberg@unimelb.edu.au or (03) 8344 4447.

Response to the Strategy Paper

Positioning ourselves for the future

Consultation Questions

1. *Do you agree with our understanding of who is responsible for managing cyber risks in the economy?*
2. *Do you think the way these responsibilities are currently allocated is right? What changes should we consider?*

In assigning responsibility for cyber security, we should emphasise the distinction between *facilitating* best practice on the one hand and taking *direct responsibility* for cyber security on the other. In many cases, Government or business assuming direct responsibility for cyber security – for example by accessing or interfering with individual devices – would potentially infringe upon individual autonomy and compromise privacy. In broad terms, the appropriate approach is for Government to facilitate good cyber security practices, thereby helping to position individuals and organisations to instantiate them, while leaving ultimate responsibility with those individuals and organisations. Some of the comments below include suggested measures that Government can take to help facilitate an environment conducive to cyber security. In addition to an essential role for Government in orchestrating incentives and consequences for poor practice, it will be increasingly important for Government to act as a role model by following best practice in the conduct of its own business.

Government's role in a changing world

Consultation Questions

3. *What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?*
4. *How can Government maintain trust from the Australian community when using its cyber security capabilities?*

Trust in Government

The Strategy Paper rightly identifies public trust as a critical component of a successful cyber security framework. Importantly, trust in the cyber security arrangements depends on much more than the robustness of the relevant technology. The Paper has a considerable focus on wellbeing as a central consideration in the development the cyber security framework, in view of the economic costs and the psychological costs of malicious cyber activity. While of course a concern for cyber safety and wellbeing is entirely appropriate, the approach outlined in the Strategy Paper would be strengthened by a bigger emphasis on individual autonomy and privacy. This is particularly important given the possible tension between these considerations: measures intended to bolster cyber security can, if not properly designed, erode privacy and autonomy. Clearer acknowledgement of the need to balance these considerations – and identifying safeguards that will help to achieve this balance - will help build public trust in the cyber security framework.

Indeed, parts of the Paper appear to suggest a significant increase in Government powers, including (for example) a potential legal basis for hacking personal devices in search of security vulnerabilities. Moving in this direction entails a genuine risk of a loss of public support for the Government's cyber security agenda. The *Telecommunication and Other Legislation Amendment Act,* as well as the issues with the 2016 Census, have arguably weakened public confidence in Government actions relating to digital security. This is further evidenced by the significant level of opt out from My Health Records. Any push for enhanced powers in the interest of cyber security is problematic in this context.

In short, there is a general expectation that, in addition to providing a framework that supports cyber security, there will be reasonable limits on Government powers to intervene on personal devices. This of course is not a comment on the current, or future, Australian Government, but a general comment on the conditions for building and maintaining public trust in the cyber security framework.

An open speech environment that encourages public engagement with these issues is crucial. The recent exclusion of a University of Melbourne researcher from 'CyberCon 2019' was disappointing. Conferences and other public events represent an opportunity for engagement with the full range of issues that are relevant to cyber security. Permitting the expression of multiple viewpoints at such events helps to build public confidence by indicating a readiness to tackle cyber security in a robust, holistic manner. The no-platforming of speakers raising privacy-related concerns can only undermine this confidence.

The current positioning of the Australian Signals Directorate (ASD) is one area that merits review. It is worth considering whether including cyber security within the remit of the ASD is appropriate. The United Kingdom has created the National Cyber Security Centre (NCSC) to sit outside of the Government Communications Headquarters (GCHQ) in order to clearly delineate responsibilities, whereas previously the Communications-Electronics Security Group (CESG) was located within the GCHQ. A similar approach in Australia may help to strengthen trust in the arrangements for defending key networks and systems by facilitating governance that builds public confidence.

The cyber landscape is unquestionably an international one, and effective cyber defence involves Australia as a player in a global system. The discussion paper could take a stronger stance on alignment with international practices, and also could profile the opportunity for Australian institutions to become a trusted facilitator for best practice, in the region and more broadly.

Enterprise, innovation and cyber security

Consultation Questions

5. *What customer protections should apply to the security of cyber goods and services?*
6. *What role can Government and industry play in supporting the cyber security of consumers?*
7. *How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?*
8. *Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?*
9. *Is the regulatory environment for cyber security appropriate? Why or why not?*
10. *What specific market incentives or regulatory changes should Government consider?*

Research and innovation in cyber security

The University of Melbourne acknowledges measures taken to help seed research activities in cyber, including the Cyber Security CRC, the Australian Centres for Cyber Security Excellence, and investments in Data61. There is also scope for cultivating an Australian industry for privacy enhancing technologies, a possibility that has been relatively unexplored at present.

However, the cyber security research and innovation system would benefit from a more open and flexible framework to build engagement between academia, government and industry. The United States' Defense Advanced Research Projects Agency (DARPA), which provides targeted investment in breakthrough technologies, may serve as a model to be adopted in Australia.

A trusted marketplace with skilled professionals

Consultation Questions

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

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

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

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

Skills shortages

As a higher education institution, the University of Melbourne is a key provider of cyber security education. We recognise the importance of this role, and that adequately responding to the needs of the labour market involves not only producing cyber-trained graduates but also ensuring that programs are appropriately designed such that our students acquire the skills needed to work in the cyber industry. Maintaining industry relevance of cyber security education programs is an ongoing challenge. The University is committed to continuous curriculum development and to deepening its ties with industry to meet this challenge. The activities of the Australian Centre for Cyber Security Excellence hosted at the University are one important signal of this commitment.

The current shortage of trained cyber security professionals is widely acknowledged, as is the need for additional cyber security professionals in the coming decade. The Strategy Paper suggests that "up to an additional 17,600 will be needed by 2026" (p.13). The University believes this significantly underestimates the number of people with cyber security skills who will be required in the development of an effective and productive cyber security industry. A flourishing cyber security insurance industry would employ several thousand specialists alone. The 2020 Cyber Security Strategy should adopt a holistic approach to skills provision, noting that many jobs that don't have cyber security in their title will nonetheless require a degree of cyber literacy. Education provision at this scale, and covering the required breadth, will involve education providers at all levels – schools, TAFE, universities and private providers.

As well as provision of undergraduate and postgraduate education, research institutions should play an increasing role in working closely with Government to help identify where future threat types may lie – as the result of increasingly sophisticated use of emerging technologies.

Cyber insurance

The Strategy Paper rightly identifies insurance as a key component of a well-functioning cyber security market. Currently, the development of a cyber insurance market is inhibited by the fact that the costs of cyber failures are largely externalised. Where companies with poor cyber security practices do not wear the cost of failure, there is little incentive for them to purchase insurance. A functioning cyber insurance market will be supported by better enforcement of the *Privacy Act* by the Office of the Australian Information Commissioner, and by fining companies, agencies and individuals for cyber breaches.

A hostile environment for malicious cyber actors

Consultation Questions

15. *How can high-volume, low-sophistication malicious activity targeting Australia be reduced?*
16. *What changes can Government make to create a hostile environment for malicious cyber actors?*
17. *How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?*
18. *What private networks should be considered critical systems that need stronger cyber defences?*
19. *What funding models should Government explore for any additional protections provided to the community?*
20. *What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?*

Responsible disclosure of vulnerabilities

The defence against malicious attacks would be strengthened by better disclosure of vulnerabilities. The Australian Government should commit to its agencies responsibly disclosing identified software or system vulnerabilities to vendors and thereafter to the broader community. This will help to reduce the number of vulnerabilities present in software and minimise the potential for development of exploits for these vulnerabilities. Google's 'Project Zero' represents a model approach.

The University of Melbourne also suggests that the Government consider legislation mandating that organisations notified of the presence of vulnerabilities in their systems respond to the notifier within a reasonable period, e.g. within 14 days. This would not involve organisations being required to divulge sensitive information but would make them responsible for taking action on identified vulnerabilities. Making businesses and other organisations more accountable for the robustness of their cyber security arrangements will make for an environment less conducive to cyber-attack.

A cyber-aware community

Consultation Questions

21. *To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?*
22. *How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?*
23. *What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?*
24. *Would you like to see cyber security features prioritised in products and services?*

Cyber education and consumer focus

While the Strategy Paper has a focus on improving cyber-awareness, we suggest it is timely to reframe the challenge in terms of 'cyber behaviour'. An increase in awareness does not necessarily correlate with an increase in cyber safety. There is a need to shift the conversation from raising cyber awareness to cyber training that has a lasting impact on the behaviour: user education should not be seen as a one-off "tick in the box" exercise. Stay Smart Online week is a positive initiative, but it needs to be expanded. By engaging communities across the country, from schools to small businesses to individual users and organisations. User education should work to demystify and simplify cyber messaging while aligning it to human behaviour and traits to assist in driving a more cyber-aware and cyber-resilient country.

Cyber-education should include a focus on what to do when attacks occur. The slow response to the Wannacry ransomware attack in 2017 indicated a lack of understanding on the part of many organisations on how to manage cyber threats.

In regard to best practice behaviour change approaches, we note that in other sectors, for example in public health and safety, there are mature and successful longitudinal awareness and behaviour change programs. These are accompanied by forms of consumer protection that include comprehensive regulatory regimes, product recall standards, and other mechanisms to balance the need for mandated protections with the demand that consumers take a level of individual responsibility. There are undoubtedly opportunities to translate key lessons from such sectors into the cyber security domain.

Contributors to this submission*

Amit Achrekar, Director, Cybersecurity, Infrastructure Services

Dr Greg Adamson, Enterprise Fellow in Cyber Security, Melbourne School of Engineering

Dr Chris Culnane, School of Computing and Information Systems

Dr Suelette Dreyfus, Lecturer, School of Computing and Information Systems

Professor Chris Leckie, School of Computing and Information Systems

Kobi Leins, Senior Research Fellow in Digital Ethics, School of Computing and Information Systems

Dr Toby Murray, School of Computing and Information Systems

Associate Professor Ben Rubinstein, School of Computing and Information Systems

Professor Liz Sonenberg, Pro Vice-Chancellor, Digital & Data and Research Infrastructure & Systems

Dr Vanessa Teague, Associate Professor, Chair, Cybersecurity and Democracy Network, Melbourne School of Engineering

Professor Monica Whitty, Chair in Human Factors in Cyber Security, School of Culture and Communication

*Note that while the researchers listed provided expert comment that informed the content of this submission, the submission ultimately represents the views of the University and not necessarily the views of individual contributors.