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

Addressed to the Department of Home Affairs, Australian Government.

2019-10-31

Note: recommendations are listed at the end of this submission.

Responses to list of questions under "We welcome your views on"

Where we are now

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

The capabilities of cyber attacks have increased over the past few years, whether that be perpetrated by nation states, non-state organised groups, criminal organisations or individuals. The capability increase is partly due to the rise in oppression-as-a-service tools marketed towards nation states, and partly due to the prevalence of surveillance devices (including smartphones and IoT devices) and consumer spyware.

The value and motivations of perpetrating cyber attacks has been increasing, partly as a result of more people using the internet voluntarily, and partly as a result of mass data collection and launching of online services (eg: the Census, My Health Record). If the Identity-Matching Services Bill is revived and passed through parliament, the identity documents (eg: passports, driver licences) of Australians will be put at risk too.

Privacy has seriously eroded to the point where many people feel helpless or have already given up on protecting their privacy. What exists now is a society of mass surveillance and surveillance capitalism, where commercial companies routinely engage in data trafficking and exploiting people's data, as well as spying on people's social media. This has been having a chilling effect on society, where people exercise self-censorship, cannot express themselves or exercise their political rights freely. This also affects people's abilities to access employment, insurance, welfare and financial services.

A particularly disturbing trend is the increasing use of biometric technologies, in often cases against people's knowledge or consent. For example, facial recognition is used at airport gates, and applied to surveillance camera footage and social media photos.

Despite this context, although data security practices have improved in some instances, government, corporate and community organisations still generally do not practise sufficient data security to keep people's sensitive information safe.

Furthermore, ironically the Australian Government has an agenda of surveillance (eg: the data retention scheme) and compromising the security of tools Australian people use in the name of "security" (eg: Assistance and Access Act 2018), further undermining the security that Australian people need. Five Eyes including the Australian Government has publicly argued against encryption and has attempted to erode encryption standards, for example by calling on Facebook to stop implementing end-to-end encryption.

Positioning ourselves for the future

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

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

I agree there is a high burden placed on individuals and small businesses to manage cyber risks. Unjust and disproportionate (relative to resources) this burden may be, the reality is individuals and small businesses collect, store and share data too, so they must take some responsibility for the data they handle.

To reduce this burden, the Australian Government should help organisations raise their cyber security practices (financial, advice, training or otherwise), and educate the public about easy ways to practise cyber security. I see the Australian Government is doing this to some extent already, such as through investing in cyber security training and provision of e-safety online resources. However, this need is ongoing.

It must be noted that technology developers and service providers have a responsibility to make their offerings secure. They should not be adding backdoors to their offerings or engaging in or facilitating data trafficking or data exploitation. Software freedom and hardware freedom (also referred to as "open source") allows the community to verify and audit technology and facilitate security fixes, but this would not absolve the responsibility of developers and providers.

Government's role in a changing world

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

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

The Australian Government could have an active role in helping organisations raise their data security practices by various means such as financial, advice, training or otherwise.

The Australian Government needs to regain trust from Australian people, not just maintain it. Most notably, the way the Assistance and Access Bill was rammed through parliament and many written submissions were ignored was undemocratic and disrespectful of technology experts, human rights groups and Australian people.

Don't hold onto 0days. The Australian Government should disclose vulnerabilities to technology developers responsibly so that they can make their offerings more secure.

Enterprise, innovation and cyber security

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

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

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

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

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

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

The Australian Government could have an active role in helping individuals and organisations practise good cyber security practices by various means such as financial, advice, training or otherwise. I see the Australian Government is doing this to some extent already, such as providing e-safety online resources. However, this need is ongoing.

Smartphones such as Android and iOS use closed-source software, which users cannot verify how it functions, and therefore cannot know whether the user would be subject to security vulnerabilities, data exploitation and data trafficking, uninstallable bloatware, backdoors and other undesirable effects. Currently, Google is in trouble for collecting location data from Android phones without users' knowledge and consent, despite some users disabling location data.

Software freedom and hardware freedom allow the community to verify and audit technology and facilitate security fixes. Furthermore, given that taxpayers' money funds public services, technological aspects of public services should be implemented with free software and free hardware to the extent possible.

The Australian Government should change its stance on encryption. An unencrypted internet is more vulnerable to cyber attacks, undermining the security of the internet and Australian people. End-to-end encryption is one security feature that can keep Australian people safe and strengthen human rights protections.

A trusted marketplace with skilled professionals

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

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

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

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

Software freedom and hardware freedom allow the community to verify and audit technology and facilitate security fixes. This can improve trust in the ICT supply chain. Although there are just few examples of free software and free hardware in commercial technology devices so far, such offerings attract software/hardware freedom advocates and security-conscious people. However, these offerings are still largely inaccessible.

Technology offerings should be based on security by design, not exploitation by design. Security features should be enabled by default, without the user needing to turn those features on, whether it be full-disk encryption, opt-in data sharing permissions, end-to-end encryption or anonymous online interactions (eg: for software updates).

The Assistance and Access Act 2018 has undermined the reputation of Australian ICT sector and the security of Australian technology. Australian ICT offerings that people previously trusted may now be compromised, and given the secrecy provisions it's impossible for people to verify whether or not that is the case. Consequently, people have been avoiding Australian ICT offerings, and technology experts have moved away from Australia. I believe repeal of the Assistance and Access Act 2018 is a necessary step for restoring trust in the Australian ICT sector.

The Defence Trade Controls Act 2012 restricts the import and export of cryptography, adversely affecting cryptography research in Australia. This law too may be keeping cryptography experts away from Australia and damaging Australia's ICT sector.

A hostile environment for malicious cyber actors

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

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

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

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

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

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

Cryptographic methods to reduce email spam (eg: proof of work) may reduce both undesirable email and phishing incidents.

Security measures of high-risk services should be revised and upgraded. For example, some mobile numbers can be ported to another carrier without the owner's knowledge or consent. An attacker could hijack a mobile number and then circumvent SMS-based two-factor authentication, often used by banks and myGov.

A cyber-aware community

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

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

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

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

The community of internet users worldwide has been demanding strong encryption, such as end-to-end encryption, HTTPS and full-disk encryption. Similarly, demand for two-factor authentication has increased. Over the years, the number of technology services that offer security features like these by default (or at all) has steadily increased.

Generally speaking, I believe the most successful behaviour change campaigns were campaigns that called on people to take simple yet effective actions. For example, in recent times, Signal is being adopted gradually by more people, due to its ease of use and end-to-end encryption being always on. In comparison, adoption of OpenPGP has been limited to essentially security experts and software developers, due to its complexity and difficulty of use.

Other views

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

The Australian Government should listen genuinely to technology experts, human rights groups and the Australian people. It was unfortunate that ACSC censored two speakers at the 2019 CyberCon conference, and pressured a third speaker to change their slide deck. These security experts should be listened to, not censored or pressured.

Technology service providers routinely avoid obtaining meaningful consent before collecting, analysing or sharing people's data. For consent to be meaningful, it must be given expressly, freely without coercion, with sufficient understanding of what is being consented to, and only by a person of proper authority (eg: an affected person or another person who can make decisions in the affected person's interests).

Some people in Australia use technology or the internet against their will, are disadvantaged or vulnerable by technology, or feel that technology as it exists today is dehumanising or unethical. Their wellbeing and concerns should not be disregarded for the pursuit of productivity, efficiency, control or political gain.

Responses to Appendix A: Progress against "Australia's 2016 Cyber Security Strategy"

24. Champion an open, free and secure internet to enable all countries to generate growth and opportunity online

Assessment
Complete

Notes
Australia champions an open, free and secure internet in a range of international forums, bilaterally and in multilateral groups including the UN, East Asia Summit and ASEAN Regional Forum. Australia has partnered with countries in the region through cyber policy dialogues to advance our advocacy of an open, free and secure cyberspace. Australia has worked with international partners to secure leader-level re-affirmation of key tenets of international stability in cyberspace including the application of existing international law and agreed norms of behaviour.

The Australian Government has not been consistently championing an open, free and secure internet, and in fact on occasions has done the opposite. For example, the Australian Government holds policies that undermine security, such as passing the Assistance and Access Bill 2018 and calling on Facebook to stop their implementation of end-to-end encryption. Internet freedom and openness has been damaged by enforcing data retention and giving a legislative knee-jerk reaction to the Christchurch shootings that instead requires a nuanced and community-driven response.

Although I acknowledge that everything in the 2016 strategy may have a deadline of 2020 and has a specific goal, championing an open, free and secure internet is generally an ongoing process, not something that can be deemed "complete" at this stage.

Recommendations:

- Stop engaging with organisations who seek to engage in or facilitate oppression.
- Help high-risk institutions revise and upgrade their security measures. One example may be adoption of two-factor authentication that is not SMS-based.
- Promote the widespread adoption and elevation of cyber security practices to a sufficient standard. Help organisations elevate their cyber security practices by financial, advisory, training or other means.
- Educate the public about easy ways to practise cyber security.
- Suspend all further migration of public data and public services to the internet, until data security practices are elevated to a sufficient standard.
- Eliminate the practices of data exploitation and data trafficking. Allow only the collection, analysis and sharing of data that consists of minimal sensitive information handled on a need-to-know basis that all people the data pertains to meaningfully consents to.
- Obtain meaningful consent from users of existing public services that are at high risk of compromise (eg: My Health Record), and delete the data of all other users.
- Oblige service providers to obtain meaningful consent from their users.
- Make it easier for people to give meaningful consent, and empower people to protect their data.
- Pay particular attention to the voices and wellbeing of people who are disadvantaged by technology or who are most vulnerable.
- Don't force people to access public services using technology or the internet. Ensure people who do not use technology or the internet are not disadvantaged.
- Disclose vulnerabilities to technology developers responsibly so that they can make their offerings more secure.
- Oblige government to adopt free software and free hardware, and encourage software freedom and hardware freedom in the wider community.
- Remove barriers to cryptography research as currently effected by the Defence Trade Controls Act 2012.
- Repeal the most draconian of surveillance laws, starting with the Assistance and Access Act 2018 and the data retention scheme.
- Approach Australian people to have an honest and sincere discussion about human rights, cyber security and keeping Australia safe.
- Add championing an open, free and secure internet to the 2020 strategy.
- Ensure that the 2020 strategy recognises the internet as a shared commons that enables human rights, and prioritises protecting its integrity and its users.