Australia's 2020 Cyber Security Strategy – Response

General Observations

The 2016 Australian Cyber Security Strategy was a positive initiative that helped Australian business understand the future direction of cyber security in this country, and we welcome the opportunity to comment on its next iteration.

As the Minister's introduction notes, Australia is facing increasingly sophisticated threats from organised crime and rogue states, which are exploiting opportunities created by the migration of everyday activities to the online environment, and the increasing connectivity of critical infrastructure to the Internet. The Strategy offers an opportunity to develop a unified, consistent response to these issues.

This response is framed from the following four-point perspective:

- The Australian Government has a unique role in two different areas of cyber security policy:

    1. The ability to build resilience throughout Australian society in the face of security threats to citizens and businesses across all sectors.

    2. The ability to develop opportunities for specialist Australian businesses providing products, services, and expertise in the cyber domain (exporters and security service providers)

- This role is unique in Australia because:

    1. All three branches of government (legislative, executive, judicial) have roles to play in defining the legal framework in which cyber exists, the way that framework is implemented, and the enforcement of that framework, which no other entity in Australia can do.

    2. Government defines the "rules of the road" for exporters and service provider businesses, and as a key consumer of these services decides which providers will be engaged with and which ignored.

- To be useful, the Strategy should make it easier for businesses to implement coherent, effective internal security programs which focus on three areas:
    - Detection of attacks
    - Prevention of breaches (attacks can't be prevented, but the ability of an attacker to cause harm can be limited with suitable preparation)
    - Response to and recovery from attacks

    This will depend on improved information-sharing between Government and business, and on increasing the trust that business and the public place in Government.

- The Strategy should also make it easier for specialist exporters to develop world-class products, and for service providers to develop a dynamic Australian-owned industry sector that provides jobs for Australians.

    Encouraging Australian ownership would increase the likelihood of cooperation between these businesses and Government, which may mitigate national security risks.

Specific Responses

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

The principle threat actors in the cyber environment appear to be the following, in order of sophistication:

- Casual attackers – low-skilled individuals who have obtained some tools and are trying them out without really understanding what they're doing

- Serious attackers – individuals or small groups with tools and the skills to use them, conducting either specifically targeted or opportunistic "target of opportunity" attacks

- Organised crime – often based in foreign jurisdictions, adopting an industrialised large-scale approach to identifying and exploiting vulnerabilities

- Nation-states – rogue nations conducting offensive operations either for political purposes (information warfare, disruption of critical infrastructure) or for financial benefit (market manipulation, extortion)

Ordinary citizens are vulnerable to all four of these threats, with better-skilled individuals able to defend themselves in line with non-cyber fraud and extortion attempts. This is also the case for the majority of small and mid-sized businesses, who do not have cyber security expertise in-house and either can't afford or don't know how to obtain assistance in the open market.

Most larger organisations with relatively mature security programs are capable of repelling the first two threats without serious problems. The ability to respond to organised crime gangs is far more variable however, and few organisations outside government have the resources to handle a serious nation-state actor.

Based on this, we propose Government adopt a multi-tiered approach:

- Continue to develop and promote the existing resources provided for citizens and small business (Stay Smart Online, ACSC Publications, ACORN, eSafety Office) – both Commonwealth and State Governments already have quality portals for small businesses addressing a variety of issues around regulation, licencing, and business development; adding links to these existing cyber resources would likely improve visibility for these stakeholders

- Continue developing law enforcement capabilities for responding to reports of cyber crime. Our experience as a business has been that appropriately-skilled police are overloaded and unable to respond to any but the most serious matters

- Work to build trust with the community – recent surveys have shown that Australians have a low opinion of Government and its role in society. This is not conducive to enhancing cooperation with citizens and businesses

- Reinforce and enhance the information sharing activities currently provided through the ACSC and the JCSCs – what's in place today is helpful, and could be expanded upon in the style of the SANS Internet Storm Center (isc.sans.edu).

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

It would be good for Government to play a larger role in providing defensive services to business – at least at a "baseline" level to maintain sensible, low-cost controls for small and medium businesses. These organisations should not need to compete on security capabilities, but on the services they offer their customers. As has been said elsewhere, customers don't look for the florist with the best security, they look for the florist with the best flowers for the right price.

This has been evidenced by Government involvement in the Energy sector, with the Australian Energy Sector Cyber Security Framework. By mandating a set of control objectives which participants must implement, the temptation to take shortcuts with protecting customer information (in the retail space) or not properly safeguarding generation and transmission assets is removed. This model shows promise and could be extended into other sectors.

Further work to demonstrate that Government actions are not simply compliant with the letter of the law, but are directed in a way which helps all Australians realise the benefits of the Internet and serve to promote the privacy and freedom of the individual will be necessary to improve the current trust deficit.

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

The current allocation of responsibility is reasonable; the way that responsibility is discharged is less satisfactory. An example is the perception that information sharing is largely one-way – businesses are sometimes reticent to supply details of detected attacks because of a belief that the information won't be responsibly shared to other businesses.

On the vendor side of the equation, there is a significant concern that legislative changes mandating so-called backdoors in encryption are undermining the ability of Australian businesses to produce world-class products, both in the security domain and elsewhere. This is unfortunate as Australia's software industry, while small, has the potential to be a significant player and source of export income in the years to come.

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

In terms of proactive vulnerability management, it's appropriate to note that Government can't "cross the border" into an organisation's network and search for vulnerabilities, however valuable such a capability might be.

That said, there are opportunities to implement passive vulnerability detection on the public Internet for a subset of vulnerabilities, building on the capability that the ACSC has already used to estimate the number of machines exposed to the BlueKeep vulnerability. Again, building on existing capabilities and enhancing relationships could be used here to allow ACSC (for example) to identify organisations that are likely to be vulnerable and proactively notify them.

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

This is a difficult question to answer, as it has significant political and sociological considerations that go beyond cyber security. It's realistic to say that many Western nations are suffering from a lack of trust between governors and governed, and that Australia is no exception to this problem, including in the cyber domain.

That said, some considerations could include the suggestions (made above) to build on existing capabilities, to enhance communication with the public, and to be seen to be acting

with the public's best interests in mind – for instance, there was a time when the Commonwealth Privacy Act was a world-leading piece of legislation, but now it is falling behind other nations. Enhancing citizens' privacy protections, in line with the EU's General Data Protection Regulation (GDPR) would be an example of this.

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

Australia's consumer protection laws are an effective means of ensuring that people get what they pay for. This could be extended into the cyber domain by legislating similar requirements for software and online services – at present a vendor can sell software without any guarantee of fitness for purpose.

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

The Government already provides some excellent resources for consumer security, however many consumers aren't aware of their existence. Better partnerships with industry could encourage communication to consumers (for example the initiative where supermarkets advertise the fact that the Tax Office doesn't take payments in iTunes cards - likewise internet service provider websites could provide links to the eSafety Office and Stay Smart Online).

Beyond that, there are opportunities to improve consumer security which require a Government response rather than a market-driven one. Two examples are establishing a minimum security standard for consumer products in legislation, similar to safety standards (this would mean, for instance, that all smart phones receive security patches for at least two years from the date the customer purchases them), and strengthening the process for porting mobile phone numbers to make it harder for unauthorised transfer which leads to identity theft.

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

A response to this question is outside our scope.

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

A response to this question is outside our scope.

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

Recent legislative changes that mandate encryption "backdoors" are inappropriate. Any "backdoor" mechanism that can be used by law enforcement can and will also be used by threat actors to compromise confidential communications and/or customer information. The end result will be a further erosion of trust in Government and of online services generally among the Australian public.

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

As mentioned elsewhere, initiatives like the AESCSF are positive because they establish a common minimum standard that businesses across an industry must adhere to – similar initiatives in other industries could be considered on a case by case basis.

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

A response to this question is outside our scope.

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

A response to this question is outside our scope.

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

A response to this question is outside our scope.

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

A response to this question is outside our scope.

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

A response to this question is outside our scope.

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

It may be very difficult to create a hostile environment for threat actors while simultaneously providing an open and secure Internet for citizens to use – certainly pressure to shift the balance in one direction risks undermining the other.

That said, improved cooperation with internet service providers to enhance detection capabilities outside private networks (assuming that internet service providers and backbone networks can be considered public), and better resourcing for police forces to respond when crimes are reported would be helpful.

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

The most common failing in identifying risks inside networks is the absence of a complete inventory of assets – most organisations of any size are unable to maintain such an inventory, and it's impossible to know what risks exist in assets that aren't known to exist. Consequently, finding ways for organisations to improve their asset identification would be helpful.

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

Networks supporting critical infrastructure, as defined by the Critical Infrastructure Centre.

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

A response to this question is outside our scope.

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

Improved trust between Government and business would be beneficial here.

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

Consumers, as a rule, don't look for secure products because they don't know that they should – and more importantly, they shouldn't have to. It should be reasonable for consumers to expect that when they purchase goods or services (for example, a new smart phone or Internet router for home) it will simply "be secure", in the same way that when they buy a heater it will "be safe".

In this sense, there's a lack of incentive for vendors to provide products that meet some minimum standard – which at this point has not been defined.

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

Australian businesses have a reputation for being innovative and producing high-quality products. If consumer demand starts to develop for secure products, the market will respond – and Australian businesses are capable of responding to this demand.

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

A response to this question is outside our scope.

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

A response to this question is outside our scope.

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

We encourage Government to keep in mind one of the goals from the 2016 iteration of the Strategy – to champion an open, free and secure internet to enable all countries to generate growth and opportunity online. Government policy is always under pressure from competing interests in this area – understandably, not everyone will see this as a worthy goal.

However, we propose that for Australia to benefit most as a community from the opportunities the Internet provides, continuing to work for an open, free, secure Internet is essential.