ABSIA Australian Business Software Industry Association

Level 5, 45 Clarence Street
Sydney NSW 2000
info@absia.asn.au | www.absia.asn.au

1 November 2019

The Hon Peter Dutton MP
Minister for Home Affairs
Cyber Security Policy Division
Department of Home Affairs
4 National Circuit Barton ACT 2600

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

The Australian Business Software Industry Association (ABSIA) welcomes the opportunity to make this submission on behalf of the business software industry and our members.

ABSIA has a compelling interest in ensuring the development of secure digital ecosystems given our members support and drive Australia's Digital Agenda. We are also interested in ensuring that everyone, including SMEs, have access to good cyber security practices.

Our key views within this submission are that:

1. The role of the Government is critical.
2. Greater attention needs to be focused on the needs of SMEs who arguably do not have sufficient resources to address security concerns adequately.
3. The Government should foster Managed Security Service Providers (MSSPs) to help reduce the burden of compliance, especially for SMEs.
4. The Government should widen the definition of "essential services" to include key financial service networks.
5. Australia has an opportunity, with appropriate and proactive Government support, to take a leading position with cyber security globally.
6. The Government should lead and encourage all entities to design and create systems and environments that are "secure by design".

For more information about this submission please contact either:

Karen Lay-Brew	Ian Gibson
Director and Head of Government Partnerships	Director and Security Lead
karen.lay-brew@absia.asn.au	ian.gibson@absia.asn.au

Kind regards,
Chris Howard
President, ABSIA

Australia’s 2020 Cyber Security Strategy - A call for views
ABSIA’s Views

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

The global cyber threat environment is becoming more complex and pervasive every day. Our cyber threat environment is no longer a localised one, but one that is global in nature and ever increasing with Internet of Things (IoT) devices and Artificial Intelligence (AI) assisted devices. This environment demands a broad but balanced approach from the Government. Focusing on specific threat areas will only create pockets of vulnerability in other areas. A broad approach is necessary to reduce the risk of cyber threats.

Historically, cyber security has been viewed as an IT specific issue. We view this as an outmoded way of thinking and are encouraged by the increasing realisation that this is now a whole of business issue. APRAs recent CPS 234[1] is a notable step in this direction with it making directors responsible for cyber security and recognising the importance of third party suppliers.

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

The current focus of responsibility seems to be on end users, and while we agree to an extent, it ignores the externalities associated with cyber risks.

The increasing interconnectedness of organisations means that the focus of cyber security is shifting from individual entities to a more holistic view of entire ecosystems. Australia itself is a part of a much larger international ecosystem. As a result, this cyber security strategy needs to recognise the importance of protecting the whole ecosystem and that the actions of one entity have flow on consequences for others.

We believe the Government has a multifaceted role to play in providing leadership and direction for the rest of our digital ecosystems. The right balance needs to be struck with the end user taking responsibility and the Government ensuring end users have access to the right information. The Government also need to lead by example.

A related issue is that there are too many entities, even within the Government, that handle security in Australia. The proliferation of Government departments and agencies with responsibility for different aspects of cyber security make it confusing for businesses, especially SMEs, to understand their role and obligations, and where they can obtain assistance.

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

Please see our answer to the question above.

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

[1] https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf

The Government has an important role to play in addressing threats, but they also have a much larger and multifaceted role to play. We have outlined these roles below.

As a business that needs to protect their own assets:
First and foremost, the Government has its own responsibility to ensure that their assets are adequately protected against cyber threats. Here, the Government should be acting as a role model and working within the ecosystem to help participants mitigate cyber threats.

In assisting ecosystem participants, the Government should take a collaborative and supportive role that sets an example for large businesses. It is too often that large organisations use cyber security as a blunt compliance tool rather than an opportunity to work with SMEs within their ecosystem to improve their overall cyber capability.

As a creator of demand for new services and the development of associated skills and capabilities through educational systems:
The Government, more often than not, introduces the need for new products and services. In creating this demand, they have a responsibility to promote the development of the necessary security skills and capabilities in the industry. Similarly, the Government should support talent acquisition and the retention of talent within Australia’s cyber expertise.

As a setter of cyber security standards that different products and services must adhere to:
The Government’s cyber security frameworks should adopt the “secure by design” concept to prevent and detect cyber attacks before these intrusions impact organisations and individuals and become breaches. This encourages secure practices and improves security across the whole ecosystem. APRA’s CP 234 is a good example of such a cyber security requirement, however it only applies to APRA regulated entities and their service providers. There may be an opportunity to implement this or a similar version to ecosystems in other industries.

It is also important to examine international standards that could perform well within Australia’s environment and consider their implementation. Using international standards expedites Australia’s ability to mature its ecosystem and allows for greater integration possibilities in the future.

As a reference for advice, education and information sharing:
While there are Government resources already available about cyber security, such as Stay Smart Online, most are not sufficiently promoted or known about. These resources should be more widely promoted and included in cyber security education in secondary and tertiary institutions.

In providing education resources, it would be beneficial to create a framework that encourages businesses to digitise and to get the basic cyber “hygienes” right. For example: digitalising, migrating to the cloud, leveraging MSSPs and so on.

There is also a responsibility to ensure that there are adequate and sufficient education facilities to deal with the evolving internal and external cyber threats.

As a policing authority detecting and prosecuting cyber criminals:
The Government has a critical role in dealing with state sponsored agents and organised cyber criminals. While this is perhaps the most widely known role of the Government when it comes to cyber security, it is still not widely understood what their powers and obligations are.

As a regulator of the cyber insurance market:
The Government has an important role in creating, stimulating and regulating Australia's cyber insurance industry. Right now, the true magnitude and impact of evolving cyber threats is still maturing and the uptake of cyber insurance is quite low. Terms and conditions vary significantly between providers making comparisons difficult and coverage problematic. On top of this, premium costs are climbing significantly. This makes cyber insurance hard to obtain and be effective. Assistance from the Government is needed to get this market right.

5. How can Government maintain trust from the Australian community when using its cyber security capabilities?
The role of the Government is not well understood by individuals and the industry. To improve this understanding, the Government needs to be more high profile when communicating about how they are preventing and assisting businesses in dealing with cyber threats and intrusions.

Legislative frameworks should also be updated more regularly to ensure that the Government can act appropriately and in a manner that is current to the digital activity of the time.

6. What customer protections should apply to the security of cyber goods and services?
The Government should consider introducing a cyber security equivalent of the Energy Rating scheme[2]. Similar to how Energy Rating labels enable consumers to make more informed choices, a cyber security rating would allow for this while also reassuring consumers about a product's cyber security level.

Please find an example of a "star rating" system below.

Star Rating	Illustrative Compliance Definition
1	● Held the 1 star rating for 12 months; AND ● No security incidents in the past 12 months; OR ● Held the 2 star rating for 12 months or more; AND ● 1 or more security incidents in the past 12 months
2	● 1 internationally recognised ISO standard; AND ● 1 Australian security standard (eg. Operational Framework)

[2] http://www.energyrating.gov.au/

2.5	● Held the 2 star rating for 12 months or more; AND ● No security incidents in the past 12 months OR ● Held the 3 star rating for 12 months or more; AND ● 1 or more security incidents in the past 12 months
3	● 1 internationally recognised ISO standard; AND ● 2 Australian security standards (eg. Operational Framework and the STN ISM)
3.5	● Held the 3 star rating for 12 months or more; AND ● No security incidents in the past 12 months
4	● Held the 3 star rating for 12 months or more; AND ● No security incidents in the past 24 months

*If a company can be upgraded to a new star rating, due to compliance to additional security standards (eg. 1 to 2 or 2 to 3 etc.), but has had a security incident in the past 12 months, the new star rating will not take into effect until 12 months have passed since the last security incident.

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

We should promote the development of cyber security skills and capabilities, including ethics training, to ensure there is a higher minimum level of security knowledge. Not only would this help individuals in understanding cyber security better, it makes them more informed as consumers. Similarly, the Government can assist in creating demand for developing consumer oriented cyber security products and services.

Implementing a rating system would also assist consumers in making more informed choices about digital products and services.

The Government and industry should also consider providing Managed Security Service Provider (MSSP) capabilities to lower the cost and capability burden on SMEs. For example, the Government could release the Trusted Digital Identity Framework (TDIF) as a service available to trusted third parties.

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

In our responses to the above questions, we have listed several opportunities that both the Government and industry can take to support a more secure environment. Below is another important piece of work that also supports secure ecosystems across the Digital Service Provider (DSP) space.

The ATO, industry and ABSIA have recently worked together to create the Security Standard for Add-On Marketplaces (SSAM)[3], which is a world first solution to improve the security of DSP add-on ecosystems. Essentially, the SSAM is an extension of the ATO’s DSP Operational Framework[4] requiring add-ons to meet a set of security requirements before they are able to connect to a DSP’s API powered ecosystem or “marketplace”. The aim is to increase the level of security across these ecosystems and better protect client data.

The SSAM is a practical way to improve cyber security across this ecosystem but it could easily be applied to similar ecosystems both nationally and internationally. The creation of the SSAM is an excellent example of the industry collectively creating recommended security requirements that will ultimately benefit all those operating in this space. It is a testament to Australia’s software industry and demonstrates our leadership when it comes to cyber security.

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

There are possibilities here but they would need oversight to ensure there are quality controls and no gaps in the services provided.

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

The regulatory environment is relatively immature and it is still evolving. As a result, it needs to be constantly reviewed. Just as there was a need to create consumer protections and rights, the same will need to be done with cyber security as we continue to transition to a digital economy.

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

This question has been left intentionally blank.

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

Ideally, digital products and services should embody “security by design” in their development meaning that all systems and environments should have both the prevention and detection of intrusions embedded within them. An example of adopting “security by design” can be found in a recent NIST Cybersecurity White Paper[5].

Standards for different sectors could be developed for products and services to be certified against. These standards could then be specified as a part of tendering requirements (initially via Government procurement) and then by the industry. The adoption of a “star rating” or similar system would assist in fostering secure software development practices.

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

[3] https://www.absia.asn.au/industry-standards/addon-security-standard/

[4] https://softwaredevelopers.ato.gov.au/operational_framework

[5] https://csrc.nist.gov/publications/detail/white-paper/2019/06/11/mitigating-risk-of-software-vulnerabilities-with-ssdf/draft

This question has been left intentionally blank.

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

There is currently a gap between the number of vacant security positions and the number of specialist security professionals available to fill them. In the short-term, we should consider reviewing visa requirements to fill this shortfall of professionals.

However, to build this market for the future, we need to start embedding security skills in all STEM education. Including security education as early as possible would help to generate interest in these career paths but also increase the minimum level of cyber security knowledge among individuals. The Government should encourage for more security related courses and education at secondary and tertiary levels to better prepare those entering the workforce.

Deakin University in Victoria has a relatively new program that is devoted to Cyber Security[6]. This may be a reference model for future education programs.

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

The cyber insurance market is immature in Australia and is facing a multitude of issues including:

- Lack of standard terms of coverage in insurance contracts;
- Small risk pools to understand risk levels;
- Difficulty in getting cyber insurance (some companies are applying but unable to get coverage); and
- Increasing premiums for those companies that are able to get coverage.

One step toward better establishing this market is to introduce clear and plain language within the terms and conditions of policies. There is also an opportunity for the Government to introduce a cyber insurance scheme similar to Worker's Compensation that would provide coverage to all businesses against a catastrophic cyber incident. This scheme could be administered by the industry and be as simple as basic coverage with the option for insurance providers to include top-up and or customised coverage.

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

One of the simplest ways to mitigate such activity is through increased education, especially for students (both secondary and tertiary) and SMEs. If more individuals and small businesses are better equipped to spot and stop malicious activity, it would help in reducing this activity.

As an industry, we could also work with technology suppliers to increase the amount of built in detection systems available on mobile and on premise devices. One example being that

[6] https://www.deakin.edu.au/course/bachelor-cyber-security

Samsung smartphones can warn users about potential SPAM or fraud attempts from certain phone numbers. There is a huge opportunity here to implement more services like this example.

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

Right now, we believe the Government's main efforts should be focused on:

- Detection and policing;
- Countering measures to originating sources of malicious attempts;
- Ensuring mandatory breach reporting; and
- Increasing active information sharing.

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

Cyber security implementations will be unique to almost all stakeholders; each government agency and private entity will have different needs to protect information. Regardless, the cyber risks are relatively similar and a joint council of government and industry representatives may be able to share themes, trends or analyses that would lead to pattern identification and better proactive management of cyber risks.

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

Many secondary networks now have the potential to create significant disruption should they suffer from a cyber incident. In addition to the concept of "unrestricted warfare", where common things such as the reliance on technology are leveraged as weapons, there are many private networks that should be increasing their security levels.

We agree that digital infrastructures require stronger cyber defences and should be included as "essential digital services". Updates to legislation should encompass these new and emerging networks that have the potential to cause significant disruption should they suffer from a cyber-attack. Networks such as the Superannuation Transaction Network (STN) and Single Touch Payroll (STP) should be included given the personal and financial data they share.

With business software, we are already working as an industry to secure the next level of the DSP network with the SSAM. Given this is a prescriptive set of requirements, it is a framework that could be applied to similar digital environments both nationally and internationally.

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

We would support the Government recovering costs through direct charges or other funding models, rather than relying on general taxation revenue. One option to consider is transaction levies. It will be important to keep in mind that appropriate funding models may vary across different networks and therefore tailored funding models should be investigated for such networks.

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

Information sharing is acknowledged as one of the best defences against cyber-crime, yet it occurs in limited situations. The main issues preventing improved information sharing include:

- Varying responsibilities across several government agencies;
- Concerns about confidentiality; and
- Concerns about commercial implications.

To support better information sharing on threats and vulnerabilities, we need to strengthen mandatory breach reporting and a collaborative culture of cyber risk sharing between trusted parties.

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

It is clear that a lack of cyber awareness is driving poor consumer outcomes. One factor to consider, is the need to increase and drive cyber security awareness from the ground up.

Currently, schools teach computer literacy, but this does not extend to the protection of information and the consequences of misuse. Better awareness about cyber security in the next generation is incredibly important as they increasingly participate in digital environments and as they enter the workforce. For example, a recent UK survey highlights that just because individuals have grown up as “digital natives” and are aware of online risks, it does not necessarily mean they aware of best cyber security practices or use them[7].

From a commercial perspective, APRA’s CPS 234 is a positive step as it formalises cyber security as a business issue that Directors have to embrace. It also acknowledges its pervasive nature by including responsibility for third party service providers.

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

Consumer awareness and focus will lead to greater demand for cyber secure products. DSPs who produce these products (with the cyber risk star rating we pose in Question 6) will have greater take up and product awareness, which will benefit businesses and consumers alike.

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

This question has been left intentionally blank.

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

Yes, this is evident in our replies to Questions 5-8.

[7] https://www.computerweekly.com/news/252472594/Over-30s-tend-to-do-better-at-cyber-security-than-younger-colleagues?asrc=EM_EDA_119658664&utm_medium=EM&utm_source=EDA&utm_campaign=20191022_Attacker%20hit%20VPN%20firm%20Avast%20through%20its%20VPN

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

The Government should continue to partner with industry organisations who represent business, software and consumer groups to extend the reach of their messages and who can provide invaluable feedback to the government before, during and after strategy execution.

The Government should also consider the pace of cyber risk as it continues to escalate. Any strategy should be reviewed frequently with the outcome being an assurance of the adequacy of all activities related to their desired outcomes.