1 November 2019

Cyber Security Policy Division
Department of Home Affairs
4 National Circuit Barton ACT 2600

By upload: https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-strategy-2020/submission-form

Dear Minister

Australia's 2020 Cyber Security Strategy

AFMA supports the Government's efforts in creating Australia's 2020 Cyber Security Strategy. AFMA's membership includes 110 firms active in the financial markets and wholesale banking. AFMA's members are highly connected, information businesses and as a result are deeply engaged with cyber security.

AFMA has been increasingly focussed on the challenges faced in relation to cyber security and has established a standing committee and held a half-day conference earlier this year focussed on the regulatory aspects of cybersecurity.

We are responding to selected questions in the consultation that are of particular relevance to industry.

Of particular note we raise concerns with the current duplicative and inefficient regulatory model for cyber security in financial services with an increasing number of inconsistent standards and multiple responsible regulators. This is far from an optimal approach.

We also raise concerns with the suggestion of cost-recovery. In our experience cost recovery is often an inefficient system that often does not conform to the government's own standards on how costs should be attributed. We also support independent consideration of whether services provided by government could be provided by private firms where this can be done more efficiently.

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: [redacted] Email: [redacted]

We look forward to continuing to be part of the process of improving Australia's cyber security.

Yours sincerely

Damian Jeffree

Director of Policy and Professionalism

Australia's 2020 Cyber Security Strategy- Consultation Responses

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

The cyber risks are constantly evolving, and it has been the experience of firms over many years that they are increasing. Firms are meeting this challenge head-on by following standards that are typically developed globally in coordination with governments and firms that are expert in security matters.

AFMA considers that the Government should be focussing on two actions:

1) Supporting businesses and end-users to lift the current standards by:
    a. Highlighting specific risks and vulnerabilities to individuals and firms;
    b. Educating individuals and firms about the general risks associated with cyber security;
    c. Creating high-profile programs that encourage more secure practices;
    d. Providing guidance to firms and individuals on how to appropriately meet existing standards - this should be done on a cooperative basis.
2) Assisting firms and industries coordinate against systemic threats from advanced actors that are beyond the capability of individual firms, such as those originating from state actors.

While we are supportive of more engagement from the Government, we are concerned there may be risks that government interventions, however well intentioned, create additional risks and costs for firms.

The discussion paper proposes "transferring responsibility for managing a greater portion of cyber risks away from end-users and onto industry and business".

While this may appear at first blush to present efficiencies, fundamentally this is a risky approach that might not be aligned with Australia's interests.

The values that underpin liberal democracies require that end-users, including individuals and businesses take responsibility for their actions and this includes managing their risks.

While these end-users are unlikely, as the paper notes, to be experts in this highly technical field, in a market economy end users will have access to such experts, and the market creates significant incentives for their use.

Moving to a model where individuals have less responsibility for their exposures also risks disengaging end users from actively managing these risks. If end-users feel permitted by the proposed change to rely more on others to take responsibility for their security this is unlikely to assist in reaching an optimum level of active interest.

The market economy approach of aligning risks with responsibilities may be in the long run a more efficient and appropriate way to create incentives aligned with appropriately managing risks.

Encouraging a culture of disengaged reliance would also likely not stop with industry and business but lead end-users to demand that government also take on responsibility to guarantee their cyber security despite the ineffectiveness of such an approach. The report notes that "Government has a limited role in protecting a large number of systems critical to our way of life". In some jurisdictions governments have assumed much greater responsibility for protection across a wide range of these types of services. However, it is not clear from the available data that this type of centrally managed approach produces more secure and resilient systems. Decentralised systems with strong individual incentives for self-protection can be more dynamic and innovative.

While governments in market economies can, of course, do more to raise awareness and support the lifting of standards, increased government responsibility of the kind proposed, is no panacea. It is likely to be high cost, may not be efficient or have the dynamism required to address the current vulnerabilities in a timely manner.

The private sector is generally more likely to keep costs down and to better align the costs with more precise targeting of risks.

Beyond decreasing welfare through inefficiency, a highly regulated approach may also present perverse incentives.

Requirements, as suggested in the paper, to require reporting of all cyber incidents would be unlikely to be of real assistance either to the firms involved, or the wider economy. These requirements increase costs and risks to firms operating in the jurisdiction. As they rely on firms reporting what they know they may also produce perverse incentives for firms to underinvest in their awareness capabilities to avoid the negatives associated with mandatory reporting.

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

Yes, from the description provided in the discussion paper the understanding appears correct.

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

These responsibilities should remain as they are. Individuals should remain vigilant on matters of security. Businesses should be responsible for their systems with the discipline of a market economy driving appropriate outcomes. Government should concern itself with advanced threats that use technology that is not publicly available.

This arrangement of responsibilities, which flows directly from the liberal democratic principles that are at the core of Australia's values, does not preclude the Government offering more assistance including proactive assistance to defend Australia's cyber infrastructure.

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

It is appropriate that Government activity is strictly regulated by law and subject to extensive external and independent scrutiny to protect the privacy of Australians as is noted in the discussion paper. Privacy including privacy from the government itself is an important freedom and one that should not be lost in order to increase cyber security.

Entities that interact with the information systems of citizens and firms should be subject to appropriate governance arrangements to ensure that privacy is protected.

The Government should focus on national security as the lens to address cyber security in balance with Australian values of being a free and open society.

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

To maintain the trust of the Australian community in using its cyber security capabilities, the Government needs to ensure it preserves the freedoms, privacy and liberties that it seeks to defend.

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

At a high level AFMA holds the Government should keep its focus on the national security related aspects of cyber security. This is the most important element of the strategy and we are concerned that the strategy may place insufficient emphasis on this broader picture, given the consumer focus of the discussion questions.

The response at present appears to aim to shift responsibilities to businesses based on consumer outcomes as a means to address national security issues. While potentially shifting the public narrative, this approach may not be an effective approach to improving national cyber security, and may diminish individual responsibility, an outcome at odds with improved cyber defence.

AFMA has supported the APRA CPS 234 standard for information security as an appropriate benchmark for ADIs to follow. We have supported this being consistently applied to firms that operate in ways connected closely with ADI functions such as through Open Banking.

This is appropriate as ADIs should follow a principles-based standard that still allows for innovation when ensuring customer data is protected.

However, we do caution in relation to applying a consumer protection approach to cyber security matters. In contrast to the APRA standard, the consumer protection framework tends towards an outcomes-based assessment. Typically, if there is consumer harm then there is a failure in the provision of the service. We have similarly cautioned against a similar approach in relation to draft ASIC Market Integrity Rules.

In areas such as information security assessing outcomes is not an appropriate approach. Even the Government has not been able to prevent breaches of highly secure systems by

state and other advanced actors. In such circumstances the application of an outcomes-based approach risks unjust results, particularly if it might be at risk over time of application without enough concern for commercial realities.

The consumer protection framework also has a punitive penalty structure of 10% of revenue which goes against the government's own recommendations in not being connected with the nature of the offence. The Attorney Generals Guide to Framing suggests "A penalty as a percentage of turnover should generally be avoided because of a lack of connection between an organisation's total turnover and the contravening conduct."1 These arrangements mean that the introduction of a consumer protection framework is likely to create large risks for firms in an area where it is difficult or in some cases against state actors almost impossible to prevent risk.

Regulating a requirement through a consumer protection framework for strengthened protections is likely to be costly, discourage the provision of services in comparison to a market-based approach where consumers are able to invest in higher or lower levels of security depending on their risk profile and appetite, and most importantly risks losing the national security focus that is appropriate to these matters.

In contrast a principles-based standard approach such as that applied by APRA to the ADI sector may provide sufficient flexibility and fairness while appropriately lifting outcomes.

The Government may also through contributions to standards bodies such as Standards Australia have a positive role to play in creating standards for particular industries in relation to cyber security, of the kind that are noted as currently absent.

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

Government should support the cyber security of consumers by supporting standards in the firms that create the products. Government should avoid a punitive approach to business, an outcome that might not be avoidable under the consumer protection framework.

Industry as the creators of the cyber security products has the key role to play in supporting the cyber security of consumers and should be encouraged to ensure the standards by which products are built are aligned with prevailing good practice.

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

Government can work with industry to support the better application of internal cyber security standards.

Industry can ensure greater compliance with relevant standards and drive the development of new standards.

1 https://www.ag.gov.au/Publications/Documents/GuidetoFramingCommonwealthOffencesInfringementNoticesandEnforcementPowers/A%20Guide%20to%20Framing%20Cth%20Offences.pdf

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

No comment.

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

No. The regulatory environment for cyber security is not appropriate at present.

We note a great deal of overlap in responsibilities in terms of which regulators are responsible for cyber security in relation to financial services. This is an undesirable state of affairs that has resulted in largely duplicative but slightly different standards and multiple regulators monitoring the same activities to different standards. For example, the APRA standard CPS 234, overlaps with the later introduced ACCC standard for Open Banking security.

ASIC is also looking at introducing Market Integrity Rules which in draft form also had significant overlap with these two other standards. These discussions are ongoing.

We encourage the use of a common standard (potentially with some specialised sections for different parts of the sector) for cyber security in relation to financial services and a single industry regulator for the standard. At a minimum there should be appropriate deference among regulators where firms are already regulated in relation to cyber security, for example where firms are regulated by APRA in their capacity as an ADI.

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

The Government should adopt a common standard for cyber security for firms in financial services. It should support firms in their efforts to meet the standard.

It should avoid a prescriptive regulatory approach and should avoid a consumer protection lens given the impossibility of avoiding some risks (noting the Government itself has not been able to avoid these risks).

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

The Government should support industry standards where appropriate for goods and services. These should be developed through the normal industry standard approaches involving Standards Australia, ISO, and other bodies.

It should not look to mandate government designed standards. This is an inflexible approach that can compromise competitiveness.

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

As per above the Government can make a positive contribution to the development of the required global standards.

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

The development of cyber security professionals in Australia is a real challenge for which there is no single solution. It likely requires prioritisation of cyber security as a specialty in education that builds on sound foundations in STEM subjects.

We note also that cyber security training needs to commence early in life so that there is widespread situational awareness of the risks.

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

Higher quality information around cyber risk practices that is referenced to standards should assist the development of the cyber insurance market.

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

The key to reducing any form of cyber-crime is through education and awareness. Cyber awareness needs to be very broadly-based within the community.

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

No comment.

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

Private or Closed User Group networks benefit from participation in structured security breach simulations and exercises, possibly industry led Red Teaming scenarios.

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

In the Australian financial services sector private networks supporting payments and settlements capabilities are generally regarded as critical systems.

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

Government is generally an inefficient and high cost provider of services. Assessments should be made by independent parties as to whether the services the government proposes to provide to industry could be provided more efficiently by the private sector. To address conflicts of interest these assessments should not be made by the concerned departments.

Cyber security is a public good and benefit flows to the community as a whole. In this regard it falls into the same basket of activities as national defence and public order. The purpose of the taxation system is to pay for these public goods. Businesses are not the creators of the cyber security threat and already expend considerable amounts of money combatting it. In many cases they are the direct victim of cyber-attacks. It is a collective responsibility of the Australian community to protect itself from this threat.

Our experience is that cost recovery programs often do not meet the government's principles for cost recovery. Given the general nature of the benefit to the community where services are provided it may be appropriate to fund them via efficient broad-based tax revenues.

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

It is recognised within the cyber security communities that the Australian government has enabled cyber-strategy, online incident reporting tools such ACORN. However, there still may be room for better and broader communication of good cyber security practices.

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

Where poor consumer choices are made this is often driven by a lack of cyber awareness.

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

We caution that approaching this issue through a consumer protection lens may have risks we have outlined above.

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

In enterprise, simulation events are good examples of a practice that raise awareness of suspicious activity. This increased situational awareness reduces risks when accessing email, online content, responding to SMS messages or phone calls.

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

The increasing scope of devices connected to the internet. Greater development of industry standards could assist in reducing the associated risks.

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

No comment.