5 May 2023

By Upload.

Dear Sir/Madam

Re: Australian Cyber Security Strategy

AFMA welcomes the opportunity to provide comment on the Australian Cyber Security Strategy.

AFMA has long been an active contributor to the development of elements of Australia's approach to cyber security, through our engagement with regulators including ASIC, APRA, ACCC, CISC as well as through our submissions to Home Affairs and others.

We see the potential for real efficiencies that would not only decrease costs for business but increase the effectiveness of the nation's cyber defences through reducing duplicative inconsistent requirements, that are often not internationally compatible, and by removing a confusing array of redundant reporting obligations.

While we have alerted regulators to these issues from the beginning of their cyber projects, not all regulators have responded optimally. While this is regrettable, we do appreciate that given the legislative and regulatory frameworks and the pressures they operate under, regulators are often driven in directions that are not always aligned with an efficient national system.

Even where regulators do take an internationally compatible, principles-based approach, and we note our appreciation for ASIC's efforts in this regard, there is a certain unavoidable level of duplication.

As such, we strongly support the work of Home Affairs to develop a more consistent cohesive national approach.

The other key to making cyber security work is to recognise that businesses are already strongly incentivised to get cyber right, that in some cases, for example those involving state actors, the challenge level can be extremely high. We encourage the recognition that an accommodative, supportive stance is the most likely to keep channels of communication and information flow open, and is most likely to support a swift uplift in standards.

The model that should be used is the same that is used in relation to air-safety, and there are many analogies between the two fields which would support the view this approach is the right one. A

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7907 Email: secretariat@afma.com.au Web: www.afma.com.au

punitive regime risks a legalistic approach to sharing risks and the benefit of experience, which would result in a far form optimal outcome.

We thank you for considering our comments below.

Yours sincerely

Senior Director of Policy

1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

AFMA would support:

- A single graded information security standard that is internationally compatible or closely linked with NIST or ISO.
- Where there is to be a reporting obligation it should be one reporting obligation only.
- Firms should not be subject to duplicative or overlapping cyber oversight by multiple regulators.
- A commitment to an accommodative regulatory stance.

2. What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?

a) What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?

Reducing duplication in regulatory schemes, moving to a regime that is compatible with international standards.

We note that already some regulatory schemes have quickly become out of date and regulators are facing large challenges to update them for cloud etc.

Particularly given the constant rapid evolution of cyber threats, a principles based connection to the leading international standards is the only approach that might be able to keep up.

b) Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

The SOCI act should avoid excessive prescription.

c) Should the obligations of company directors specifically address cyber security risks and consequences?

Company directors already have responsibility for cyber security risks and consequences. Regulatory proposals in relation to director obligations around cyber security often place management type obligations on what should be a governance body. We suggest the current arrangements are appropriate.

d) Should Australia consider a Cyber Security Act, and what should this include?

A Cyber Security Act could reduce duplication with a specialised regulator with the technical expertise to maximise the assistance to businesses to lift cyber security standards.

e) How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?

As noted above there are substantial opportunities to streamline existing requirements by moving to a single national system that is compatible with international standards such as NIST and ISO.
At present multiple regulators will inspect or audit the same firm for similar requirements. A single firm might have to present to APRA, ASIC, ACCC and SOCI. This is costly and wasteful.

To monitor the regulatory burden the Government should conduct externally run surveys of businesses to assess costs.

f) Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by:
   a) victims of cybercrime; and/or
   b) insurers? If so, under what circumstances?
      (i) What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?

We note the risk of creating undesirable incentives in this space around which targets are selected and advise caution.

g) Should Government clarify its position with respect to payment or nonpayment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

As above.

3. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?

AFMA supports working with neighbouring jurisdictions to build cyber resilience and improve responses, this could include promoting a common approach to standards.

4. What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?

Australia could look to work with leading jurisdictions to leverage their expertise and standards. This might involve contributing to common standards, rather than developing similar standards locally.

5. How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?

In relation to standard setting contributing to international standards is more likely to keep standards current and at the technological level they need to be.

6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

No response.

7. What can government do to improve information sharing with industry on cyber threats?

No response.

8. During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?

This might be of assistance. We note that in a punitive regulatory regime there may still be risks with sharing information.

9. Would expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?

No response.

10. What best practice models are available for automated threat-blocking at scale?

No response.

11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

No response.

12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

No response.

13. How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians? a. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

This would be of benefit but again we query the efficiency of having multiple non-specialist regulators overseeing cyber security in a duplicative fashion.

14. What would an effective post-incident review and consequence management model with industry involve?

We encourage the Government to adopt the air-safety approach to incident response. Further government involvement in firms' internal processes is unlikely to be of benefit.

15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime? a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

No response.

16. What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

There are a wide range of activities that could assist particularly smaller firms keep pace with cyber challenges.

17. How should we approach future proofing for cyber security technologies out to 2030?

AFMA would advise:

- Using international standards that are more likely to stay up to date.
- Keeping requirements principles based.
- Avoiding a prescriptive approach which risks locking in technologies.
- Ensure costs to business are managed so that cyber security budgets are not overwhelmed with regulatory costs.

18. Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?

No response.

19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

No response.

20. How should government measure its impact in uplifting national cyber resilience?

The Government should commission studies by independent parties periodically to measure progress.

21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

No response.