SUBMISSION TO INDUSTRY CONSULTATION ON THE AUSTRALIAN CYBER SECURITY STRATEGY 2023/2030

Dr Malcolm Shore
Offsec APAC

The Challenge of Cyber Attacks

The discussion paper highlights the Optus and Medibank attacks in 2022, and notes that the Government was ill-prepared to respond. In terms of the Cyber Strategy, we would observe:

- First, response is what happens after a target fails to protect it's assets.We would suggest that a more effective approach is to defeat the attack through protection, and so not necessitate a response. This requires an architected set of preventative controls. We should focus, in NIST terminology, on IDENTIFY and PROTECT, not RESPOND and RECOVER.
- Second, it is not the government's role to respond, but the agency's role. Government should focus on good governance by ensuring that it has visibility of the risk and can ensure risk mitigation.
- The value of increased regulatory instruments is somewhat questionable. Despite the implementation of the Telecommunications Sector Security Reforms, the Optus attack (and many others since TSSR was enacted) would suggest that compliance is not an effective approach to achieving real data security. While compliance is necessary, we would suggest that having cyber staff skilled and experienced in defending against attacks is a better strategy than cyber staff skilled in completing regulatory checklists.

We note there is a blending in the discussion paper of cybersecurity as a national revenue stream and the losses due to cyber attack. We believe the latter issue cannot be addressed adequately by introducing more security devices into our networks - the underlying causes of data breaches require some fundamental changes to the paradigm of cyber defence. There may well be an opportunity to grow the cyber products industry but this is a quite different issue from that of protecting the nation, its industry, and its peoples.

While implementing more effective cyber defences to protect against increasingly sophisticated nation state cyber attacks is necessary, this can only be a short term element of the strategy. An ever increasing cyber arms war against adversaries with substantially more resources arrayed against us cannot be sustainable into the future, and we must look for ways to work globally to reduce the threats at source through longer term strategic objectives such as enhanced cyber diplomacy, more effective global network designs that can deliver full attribution, and trustworthy technologies that deliver resilient systems.

Specific Response to Questions

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?

We would like to see a Government-led initiative to promote (by example) the use of Penetration Defenders, a cadre of skilled cyber defence operators capable of not only understanding cyber attack techniques (in the same way Penetration Testers do), but who are demonstrably skilled at protecting against them, detecting them, and defeating them. Rather than focus on standards and best-industry compliance we would encourage a pivot of resourcing to active and capable defence and measurement of an agency's ability to defend against attack.

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

a. 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?

We would suggest further reform to this Act in order to gain visibility into the risk to critical infrastructure services, and one way to achieve this would be to leverage the existing STIX/TAXII solutions for threat intelligence to deliver integrated risk reporting for the national critical infrastructure. Please refer to our pre-publication research paper submitted under separate cover entitled “Improving Cybersecurity Risk Management for the national Critical Infrastructure”.

We would suggest strongly that more checklist regulation be avoided, and that the focus turn to public-private partnerships for operational testing of cyber defences. This could be through government run unannounced red team activity or pre-announced cyber drills. Any regulation would then focus on the obligation to remediate weaknesses.

b. Should the obligations of company directors specifically address cyber security risks and consequences?

At the Board level there are no cyber risks, just business risks. There should be no special call out on cyber.

c. Should Australia consider a Cyber Security Act, and what should this include?

No comment.

d. 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?

A higher regulatory burden of checklist compliance should be avoided. Some level of tax relief should be available to offset investment in cyber defence skills (not products) to mitigate the regulatory burden and provide visibility, and any increased regulatory obligation should be in the form of passing an operational test of defences.

e. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals

We would not support prohibiting payment of ransom. Prohibition would lead to the majority of attacks not being reported and for those that are there would likely be an adverse economic impact on the businesses. It would have no deterrent effect on cyber criminals.

f. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?

As above.

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?

The UN ODA cyber norms provide a useful vehicle for establishing a common understanding in support of cyber diplomacy. This initiative includes outreach to support developing nations in building their cyber defences and resilience. Australia could usefully take a regional leadership role in encouraging activity in support of the UN ODA cyber diplomacy initiative.

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

As above. In addition, further support for multilateral academic research would enable innovation to improve cyber resilience while elevating Australia's international leadership through research partnerships.

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?

Through promoting by example the work of UN ODA on cyber diplomacy, including international outreach to developing nations.

Through increased commitment to supporting standards setting bodies through public-private partnerships.

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

As noted early in this submission, we would like to see a Government-led initiative to promote (by example) the use of Penetration Defenders, a cadre of skilled cyber defence operators capable of not only understanding cyber attack techniques (in the same way Penetration Testers do), but who are demonstrably skilled at detecting and defeating them. Rather than focus on standards and best-industry compliance we would encourage a pivot of resourcing to active and capable defence and measurement of an agency's ability to defend against attack.

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

No comment, other than noting the existing STIX/TAXII solution provides an operational level of information sharing.

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?

No comment.

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?

We would suggest the focus be on preventing attacks rather than recording failures.

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

No comment.

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

The Certificate IV in Cybersecurity has provided a significant channel for delivering operationally-ready cyber skilled staff. This initiative could usefully be tailored to better vet potential students, ensure a lower drop out rate, and ensure graduating students are highly skilled. The TAFE model of vocational training can be further developed by enabling recruitment and retention of suitably skilled tutors through some form of salary supplement.

There are many cyber academies being spawned in industry to take advantage of skills shortages. A national Information Resilience program spearheaded by ACSC and with cyber academies being encouraged to become partners would ensure a common and adequate level of training. (As exemplified by the Information Assurance programme launched some time ago in the US)

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

As above.

With a global shortage of cyber security skills, getting skilled immigrants for cyber security will continue to be challenging. Ongoing improvements to visa and citizenship opportunities would assist.

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?

We would suggest the focus be on preventing attacks rather than recording failures.

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

We would suggest the focus be on preventing attacks rather than recording failures.

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

The Government could through its small business grants encourage businesses to improve their ability to protect their assets from cyber attack. For example, this could take the form of requiring evidence prior to acceptance of a grant submission of attendance at a public-private partnership training seminar provided by AISA; or of having engaged a suitably qualified and government accredited team to provide a Penetration Defence Test; or having a suitably qualified cyber security manager.

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?

As covered above.

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

Continuing investment in the Cybersecurity CRC, with a research stream focused on cyber resilience in the context of technology trajectories (eg quantum crypto, 6G, etc).

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?

This question assumes that more companies providing more products and services is good. However, more of the same is by no means a silver bullet for security. There needs to be a clear strategic vision of what cybersecurity effectiveness looks like before encouraging cybersecurity firms to just build more boxes. Clearly Government can lead by example through procurement, but it needs to very clearly understand what is required to be fully cyber secure before assuming that Government can set an example to others. The continuing breaches of government systems would argue that more work is required before Government is in a position to be the "gold standard" for cyber security.

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

Aerospace has come a long way (albeit with an occasional glaring exception) in ensuring its flight technologies are secure and resilient. This sector is an example of what we can already do to provide secure systems **if we have the will**. The approaches taken by Aerospace provide good learnings, albeit with a cost in much better trained developers and more trustworthy development environments. Software vendors are able to disclaim all responsibility for beaches via their EULAs, and there is no lever to force them to build good, trusted software. Given that the vast majority of software is from overseas sources, trustworthiness will be a long term problem. Ensuring Secure-by-Design is included as a mandatory component of the programme for any Government-funded cyber academy would be a good start.

A *tickmark program* (as promoted by the IoT Alliance Australia for IoT devices) would also provide a level of assurance through testing. However, we note the failure of the AISEP scheme to achieve any significant benefit to the digital economy - any tick mark program needs to be fit for purpose.

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

National cyber resilience can be measured in terms of risk. We would suggest two approaches. Firstly, as per the referenced pre-publication research paper we would encourage the adoption of a common approach to measuring the maturity and effectiveness of an organisation's cyber security processes. Secondly, as mentioned earlier, the adoption of a CARR/TAXII approach to gaining central visibility of risk is suggested.

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

No comment.