2023-2030 Australian Cyber Security Strategy
Response to discussion paper

14 April 2023

I appreciate the opportunity to contribute to this important discussion and welcome further dialogue on the topic.

https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/2023-2030-australian-cyber-security-strategy-discussion-paper

I provide this submission as an individual with a background in Technology and Financial Services (both as an Executive and an independent Non-Executive Director), ***not*** as a representative of any particular organisation. I have elected to comment only on matters where I feel qualified to provide an opinion.

Rob Hale

Question 2c - Should the obligations of company directors specifically address cyber security risks and consequences?

Applying to regulated financial services organisations today, CPS 234 is an existing prudential standard that explicitly highlights board responsibility for information security. As a company director and a technology executive, I am aware of the breadth and complexity of cyber security as a topic and the challenges this obligation creates - even for mature organisations within a well-regulated industry.

While it may create focus and give attention to an important topic, I am hesitant to suggest that the obligations of directors should specifically address cyber security risks and consequences. Rather, clear and consistent government advice and support seems a better route to improving the approach and responsiveness of boards on cyber security matters.

In the first instance, government focus on provision of support for directors on boards of critical infrastructure providers may be beneficial.

In the event any new obligations are introduced, a phased implementation approach should be considered. This would allow for board succession planning and provide existing directors with an opportunity to supplement their skills if required.

Question 2g -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?

Yes, this would be helpful.

At present, this is a confused area and a topic of ongoing debate at board level with significant effort being expended on a national scale. A definitive statement on the legal position and any related conditions or constraints would provide much needed clarity. This is particularly the case where consideration of ransom demands is urgent and the materiality of private information at issue is significant. This position can of course change over time as new threats emerge and legislation is introduced.

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

While attacks typically target an industry or set of businesses within a country, cyber threats do not respect conventional borders. Techniques are constantly evolving and once proven to be successful, an attacker may broaden their radius. Establishing mechanisms to share the knowledge and experience of such attacks, their impacts and methods to combat effectiveness could lessen the impact in other jurisdictions. This is not dissimilar to existing methods used to share information between financial institutions about payments fraud and other financial crimes.

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

Government could facilitate access to a central team of cyber security experts well versed in the management of incidents and with visibility of recent and ongoing attacks. These experts would also be able to maintain and direct enquiries to the latest government guidance and recommended best practice response. This could extend to related topics such as media announcements and customer communications, including social media. Consumers could benefit from receiving updates in consistent, simple, clear and unambiguous language developed specifically for this purpose.

This same function could support early secure communication to other critical infrastructure providers, advising them to be on notice for particular forms of attack, potentially strengthening their own security measures.

For Australian businesses, being able to rely upon a standing arrangement to contact pre-vetted experts at short notice would seem to offer value and could save vital time determining how best to respond in the early hours of an attack.

Question 8 - During a cyber incident, would an explicit obligation of confidentiality upon the ASD, ACSC improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASC/ACSC without the concern that this will be shared with regulators?

This suggestion seems defensive and based on an assumption that organisations should be protected from regulators. Given that regulation exists to protect Australian consumers and businesses, failing to notify regulators of cyber incidents would appear to be inappropriate and counter-productive.

On the assumption that regulated companies are prudently governed and conduct legitimate business practices with fit for purpose operations, they should have nothing to hide from a regulator. Perhaps a shift in cultural and public perception is required when such organisations become victims of a cyber attack.

Question 9 - Would expanding the existing regime for notification of cyber security incidents improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?

Broadly speaking yes, however there are already a range of pre-existing notification obligations for Australian businesses today. These include OAIC, APRA, ASIC and ACCC. Timelines and related actions vary and create complexity for Governance and Compliance teams. It would be helpful if these could be consolidated and notification could be made just once to a single government agency with a single set of agreed obligations and timelines.

Intra-agency access to a centralised set of notification data could also improve accuracy and support more comprehensive and flexible reporting which in turn, could help identify trends and emerging risks more readily.

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

See above response to Q7

Additionally, the idea of accreditation is interesting. We should draw on recent learnings from the Consumer Data Right (CDR) Data Recipient accreditation process. CDR provided a set of prescribed information security capabilities as part of the legislated rules that proved to be a barrier to participation for many. If the goal is to elevate collective capability then a good early outcome would be provision of an accessible framework and resources that *encourage engagement and participation* in the topic. Even small incremental improvements will strengthen Australia's overall capability.

Question 13a - Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

Yes, see above response to Q9.

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

Drawing once again on recent experience with CDR, it may be better to recognise and acknowledge that we do not know what lies ahead. We can and should plan based on what we know today yet embed flexibility into our strategy and associated tools and frameworks so that we can rapidly adapt and adjust to changing conditions. The very nature of cyber security means it cannot be future proof.

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

It is great to see the need for metrics and measurement being recognised and considered at this early stage. Without measurement, we cannot determine if we are making progress or whether particular initiatives are materially contributing to a desired outcome.

Effort should be made early on to define a measurement mechanism that reflects the initial state and progress towards the desired end state. This could be achieved through establishment of a benchmark - potentially one that could be used globally to assess resilience. The definition of such a benchmark or assessment tools will depend on the objectives of the strategy (see Q21 below).

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

We should have a clearly defined desired future state or outcome - a north star to help ensure all strategic effort is appropriately focussed and enhancements and extensions to the strategy are in keeping with the overall agreed objective.

Once defined, a series of initiatives and capabilities can be determined that collectively support progress towards the objective.

To assist with *how* these capabilities are progressed, we should establish a set of guiding principles.

Once all of this is in place, two sets of metrics can be explored. The first set will help track implementation progress for the specific initiatives and capabilities. The second set will help assess the level of capability that results from these. Ongoing regular assessment will be required to ensure that progress continues to be made in the right direction at the desired pace.