2023-2030 Australian Cyber Security Strategy Discussion Paper - Sezoo's view

Summary

Sezoo is delighted to have the opportunity to respond to the 2023-2030 Australian Cyber Security Strategy Discussion Paper.

We support the Minister's stated focus that Cyber Security should create a digital environment that is "safe, trusted and secure". As an Australian company founded on a mission statement to "radically improve trust in digital interactions for the benefit of all", this focus resonates strongly with us.

Recent local and global events have made it clear that cyber security is one of the many pressing concerns of our current age. We agree with the paper that "our national resilience, economic success and security rely on us getting our cyber settings right". To this we offer a few observations:

1) In our efforts to make things secure, we must not destroy the very things we seek to protect. Cyber Security, like most things, is a complex system of checks and balances, trade-offs and compromises. It is not "binary", nothing that is of any use can be 100% secure. We must not be so secure that we cannot enjoy our freedoms.

2) Centralisation of data, services and "intelligence" can be attractive, but increases the value and reducing the number of targets for bad actors to focus on. The design of data holding, processing and sharing solutions should look to reduce centralised patterns and enable dispersed and/or decentralised patterns to reduce the value of targets and the attack surface.

3) Resilience is well chosen as a term. To be resilient means that we are able to continue even if faced with set-backs. This demands a broader mindset than terms such as "secure" or "protect". Resilience demands that we allow for the possibility that things will fail and asks us to consider what we will do to "carry on" when they do fail.

This thinking leads to our key recommendation for the discussion: Australia's Cyber Security Strategy must consider how to create a digital environment that is not vulnerable to the failure of any one piece, system or organisation. We must not create a fragile system as an unintended consequence of our attempts to protect the status-quo. "Hardening" and making things "robust", while sensible in isolation, do not make the overall system "resilient", for this we need a strategy that is "anti-fragile" (as coined by Nicolas Taleb).

Finally, we have also recently provided comments on the Privacy Act Review Report and recognise, as described in the paper, that the Australian regulatory framework has several areas of overlap and shared interest. We support the call in the discussion paper that the regulatory framework be streamlined and simplified as far as possible. We see complexity in these related spaces as adding to the risk of unintended non-compliance and the deliberate cherry picking of preferred regulatory interpretations.

We took the opportunity presented by this review to share and exchange our thoughts with our colleagues in the 460degrees Cybersecurity Team. Their review takes particular interest in the human centred cybersecurity issues (an area of deep expertise for the team).

We have provided our specific Sezoo responses to the questions amongst the 21 for which we have expertise.

As citizens and business founders in Australia, we wish this initiative well in its intent to provide a safe, trusted and secure digital environment.

John Phillips Co-Founder Sezoo	Jo Spencer Co-Founder Sezoo

#	Discussion Paper Question	Sezoo Response
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 strategy that aims to minimise single point sensitivity to failures and minimise targets (and the resulting harms due to breaches) for bad actors. To this end, if we are able to minimise the fraudulent benefits of having sensitive information (of knowing things ”about” people say), then the incentive for data breaches would be reduced. So, in addition to addressing perimeter and access security, the focus for solutions and ecosystem designs should be to specifically authenticate individuals and systems access. We shouldn't build systems that assume that knowledge of accessible information (user names, emails, etc.) means that you must be that person. We should all aim to protect ourselves and the organisations that we are a part of as well as possible, however reliance on any single system and/or single access or service point, no matter how “strong” we make them, creates fragility and amplifies the risk that one failure will lead to a systemic failure. We need an “anti-fragile” strategy, not (just) a strong citadel strategy. This is the design principle, and objective, of the original internet. Without including “anti-fragile” thinking, our efforts to strengthen the defences of existing systems risk making us all more fragile to attack.

#	Discussion Paper Question	Sezoo Response
2	What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?	The discussion paper provides an initial view of the related legislative initiatives currently under consideration. Having just completed our comments on the Privacy Act Review Report it is clear just how inter-woven the security related/aligned frameworks have become. We agree that we need reforms, and we also agree that these need to "simplify and streamline existing regulatory frameworks." To this we would add that complexity created by having multiple overlapping frameworks significantly increases the risk of non-compliance through mis-understanding as well as cherry picking or deliberately choosing the "easier" path rather than the most secure path. In addition, the digital technology that supports our social and economic lives is ever evolving, as is the technology and social techniques used to exploit weaknesses in our digital environment. Whilst we should be mindful of emerging threats such as the mis-use of AI, Web3 etc, we must not embed technology specific solutions and approaches in the regulations. The application of technically agnostic regulations should be considered as guidelines and enforced as policies and practical accreditations.
2a	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)?	No comment, not our area of expertise
2b	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?	No comment, not our area of expertise
2c	Should the obligations of company directors specifically address cyber security risks and consequences?	Yes, and we would suggest that this consideration look at other related regulation such as the Banking Executive Accountability Regime)
2d	Should Australia consider a Cyber Security Act, and what should this include?	No comment, not our area of expertise

#	Discussion Paper Question	Sezoo Response
2e	How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cybersecurity, and are there opportunities to streamline existing regulatory frameworks?	No comment, not our area of expertise
2f	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?	No comment, not our area of expertise
2f-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?	No comment, not our area of expertise
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?	No comment, not our area of expertise
3	How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?	No comment, not our area of expertise
4	What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?	No comment, not our area of expertise
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?	No comment, not our area of expertise
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 comment, not our area of expertise
7	What can government do to improve information sharing with industry on cyber threats?	No comment, not our area of expertise

#	Discussion Paper Question	Sezoo 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?	No comment, not our area of expertise
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?	Yes, in general, but this may become a double edged sword in extreme circumstances. While we are advocates for transparency, if there was a crisis we would need to be careful that we don't overshare information about issues and create panic and/or information overload. In addition, the combination of penalties for not meeting cybersecurity regulations, and the demand for notification of incidents can create conflicting tensions. Where possible, notification needs to be encouraged and not be directly associated with penalty. Lessons should be taken from existing notification and reporting regimes (such as AML/CTF reporting)
10	What best practice models are available for automated threat-blocking at scale?	No comment, not our area of expertise
11	Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?	From our perspective we would ideally like all people to be aware of cyber security from a personal view. In addition we will need an increased number of professionals who have up to date knowledge of cyber security measures and counter-measures. However not all people can be experts and there are many topics in which we need expertise, not just cyber security.
12	What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?	Both encourage further (and continued) education and prevent people masquerading as qualified if they are not. Provide a framework in which certified professionals can prove their certification to their prospective employers and clients.
13	How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?	Take any/all lessons learnt from the COVID 19 response (both what worked, and what didn't work). For example, a key initiative that was often cited as working well was the regular meetings of heads of state and federal government.

#	Discussion Paper Question	Sezoo Response
		Equally, it was often cited that differences in the actions across state/territory and federal government borders created confusion and frustration.
13a	Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?	No comment, not our area of expertise
14	What would an effective post-incident review and consequence management model with industry involve?	No comment, not our area of expertise
15	How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?	No comment, not our area of expertise
15a	What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?	No comment, not our area of expertise
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?	Recent developments in "verifiable credentials" (such as the W3C Verifiable Credential Data Model standard and the ISO mDL 18013-5 standard) and the use of cryptographically secure decentralised interaction models offer offer ways in which we can create more resilient proofs of things about people, organisations and things. Note that we are not proposing the use of "blockchain" or "Web3" based architectures - the use of these technologies can bring some benefits, but also comes with some risks (as do all technologies). The Verifiable Credential based model and decentralised interaction patterns offers one of the ways in which we think a more resilient, a less fragile, less-attractive target digital environment can be achieved for Australia and Australians.
17	How should we approach future proofing for cyber security technologies out to 2030?	No comment, not our area of expertise
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 comment, not our area of expertise

#	Discussion Paper Question	Sezoo Response
19	How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?	No comment, not our area of expertise
20	How should government measure its impact in uplifting national cyber resilience?	No comment, not our area of expertise
21	What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?	No comment, not our area of expertise