2023-2030 Australian Cyber Security Strategy Discussion Paper

Reference: 2023-2030 Australian Cyber Security Strategy Expert Advisory Board

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?
   Cybersecurity labelling for commercial products sold in Australia that are internet connected, similar to Food Regulation 2015.
   Public and trustworthy (transparency) Cyber Hygiene Services, similar to; CISA's Vulnerability Scanning (VS) OR; NCSC Web Check. Australia's scanning is obscure, opt-in and unknown, and our CHIPs report is insufficient for this goal
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)?
      In terms of 'mandatory' it would be a good start to make anything actually 'mandatory'. There are plenty of legal levers in Australian cybersecurity standards coming out of the ASD, ACSC, OAIC, ACCC, but there are no 'teeth' unless the issues fall under regulators such as ASIC AHPRA APRA etc.
      Australia has some of the worlds most stringent and effective cybersecurity policy, standards, guidance, and frameworks BUT they are useless or rendered useless through exclusions and weasel words that allow almost all organisations a way to avoid repercussions. If there were less exclusions and less use of weasel words in the Acts we have, there would be actual real world repercussions because accountability could be escaped in fewer circumstances
   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?
      In terms of 'definitions' it is quite clear, the issue is not with the written elements of the Act, it is with education and oversight, Australia has a lot of great 'literature' written but it is not useful for the desired outcomes until better oversight and education is introduced to put into reality what has been written in the Act
   c. Should the obligations of company directors specifically address cyber security risks and consequences?
      Australia has an opportunity to better understand the reality of businesses and their realistic capabilities in the Australian society and government - before jumping to conclusions about who in these businesses can be held accountable. It would not be very logical to hold the mechanic accountable for your car damage when you were drunk driving and speeding because the mechanic was the last to maintain he break pads that failed to stop your car in time. That is what is sounds like to a cybersecurity professional who hears politicians and media speak about director liability for things that they could never possibly have changed in the first place - cybersecurity incidents WILL happen and if the director is accountable I would expect that their motive and negligence be proven when a piece of software is inadvertently released without proper security controls that an automated attacker controlled piece of software uncovers it to lead to a malicious actor to commit computer crimes leveraging the unintended act of a software developer. Yes the software was created by the company for which the director is responsible, but the incident occured because an attacker coded a bot then committed a crime, act of the

criminal was not a motivation of the director or their staff. The cloud service provider gave the director confidence about the security of the cloud they used, and the organisation is in a country that monitors for internet connected software with security flaws but the government did not notify them of the issue either. So did the cloud provider fail, the government, the software engineer, or the director in charge? Where does the bad actor fit in here, without them there is no incident inherently.

Australia should take this rare opportunity to better understand companies' challenges, where they put their trust, and where that trust fails them. Perhaps they should not trust cloud service providers, perhaps they should not trust the government who are supposed to be monitoring their public attack surface.

And maybe the law to hold directors accountable should account more for their intent and reality of what is possible when they are being judged for cascading failures all around them they can not possible control or even feasibly influence - and should not be expected to by law - we will only turn away directors and discourage educated and informed people who know they will be in an impossible position, leaving only uneducated directors who are ignorant to the impossible situation the law puts them in.

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

Australia should take this rare opportunity to develop a Cyber Security Act, we should develop it with the scope of the entire planet and interplanetary use cases that Australia has interest in the use of cyber-communications (public/private shared communications across the universe). That is what any Act must consider, Cyber Security has no concept of Australia, unless we are going to legislate physically at the level of routers and switches - which would make the Act a reform of telecommunications Act governing the ISP's and ensure they are applying better security measures to protect Australian's at our physical cyber-borders!

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?

Australia "seek to monitor the regulatory burden on businesses". Let's unpack that one at a time. Stating the obvious here, maybe hold back any activities until you first understand "regulatory burden on businesses" by actually trying to set up a regulatory capability that is more appropriately funded and enabled to be capable of being a regulator. I would imagine regulatory burden on business is a direct result of Australia being unable to actually conduct any effective regulatory activities across the industries it regulates putting undue burden on business that should be part of the regulatory oversight as a government service itself.

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?

Stating prohibition inherently means consequences for making a payment. If the option is pay or health and safety, and payment is prohibited, the law that prohibits it would be responsible for the unavoidable health and safety harm as the only viable indirect result. So while I as a human can easily identify prohibition folly, I do agree prohibition may be necessary because funding criminals incentivises more criminal activity and harm. The only way is to balance harm versus deterrent, and many solutions come to mind; the easiest would be an authority to pay, which needs to be timely and having a low barrier also means it will be a potential for abuse and defeat the intent of the prohibition. Another option would be prohibition but allowing payment in health and safety situation that has a limit payments BUT that is eventually going to be well enough known that criminals would change tactics to target organisations that can pay and not those who are prohibited resulting in more harm than we have now. There are also options involving insurers, brokers, or international parties who pay on behalf of Australian business that would avoid any prohibition in our laws. Criminals by definition do not care about the laws we decide on and would attack for payment anyway, and expect the victim to pay regardless if the victim can legally pay or not, then we are doing law enforcement against victims who pay instead of law enforcement against the criminals - so I see no good options other than avoiding laws that further victimise victims, by strengthening laws to help law enforcement against the criminals directly.

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

3. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?
   Regional in this context is an oxymoron, as described in 2.d cyber has no borders, borders fall under ISP's and reform of telecommunications act can provide pseudo borders on cyber for Australia to govern. Beside governing these border devices and the companies operating and powering them, Australian government would have only the word regional and not the meaning of the word in reality. So to answer this more directly, work with the neighbours at the level that governs the devices, satellites, and sea cables that make up Australia's cyber-borders.
4. What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?
   Covered above, and consider extending it to NATO to form consensus on devices, satellites, and sea cables that make up NATO member imaginary cyber-borders. This will hopefully unite us in common purpose and shared realisation of that unity, like never before
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?
   Covered above, cyber space definition literally means an imaginary space without limits, therefore the question seems repetitive and less relevant when you consider the national stage and role of NATO
6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?
   There are 'best practice' for as many distinct business types combined with the numerous ways to practise business. No single set of 'best practice' applies to more than one business, or a better way to say it is one business 'best practice' will not suit any other business. What might be misunderstood by the author of this is something referred to as the 'baseline' which is a collection of foundations for which all practices are built upon. These foundations are the concrete under your house, the best house for you is built to your needs and the same is said for business best practices. So what we need to establish is an essential maturity model (we have one already) with many optional pathways from the foundations concrete slab to build you own cybersecurity maturity house upon (we have these too). The challenge is not what the question asks, the challenge is in having business apply the foundations are the baseline and which elements like beams, power, and plumbing to put in their home - with the ability to enforce these building requirements so we don't have homes/businesses burning down due to negligence as often as we are now.
7. What can government do to improve information sharing with industry on cyber threats?
   It is already a great publisher of actionable advisories, it is already sharing. Businesses require assistance in how they might consume and use what is being shared, and many business likely unaware of the shared intelligence. In many cases the sharing is done in closed forums,

paywalled, or exclusive - this is anti-sharing and while i have benefited greatly for what is being shared in those contexts, it is obvious to me that is not true sharing and most businesses never benefit at all even if they are aware these exist because they're not credentialled, eligible, or funded enough to be part of them

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?
   Yes, and telling stories about how this helps the Australian business community so it is seen as a benefit and not a business risk to share. We need to provide confidence through education that sharing is not going to put the crosshairs of law on you like it does in other legal contexts like tax where being forthcoming can put you in jeopardy of some losses or undue burden to defend yourself.
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?
   These are the details that are best described as results of cybercrimes, like the sale of stolen goods at a legitimate secondhand store is an outcome of a theft crime, ransomware and data extortion are the result of phishing and/or malware and/or using exploit payloads for malicious purposes.
   If any initial incident occurs and the initial act did not result in a successful conclusion of an attack like ransomware of data exfiltration and extortion - then these criminal acts and incidents go unreported today! The existing regime for mandatory notification should not exclude criminal acts that are security incidents that failed, because the next target may not fail and the lack of notification of failure may be the cause of future harm BECAUSE it was not a notifiable incident.
10. What best practice models are available or automated threat-blocking at scale?
   Both are imaginary, they cannot exist. See point 6 about best practices. automated threat-monitoring and alerting is not imaginary, the part making it to scale requires skill analysts to take the rich and non-false positive alerts and perform business specific remediation that may be blocking. The challenges for scale are two fold; 1/ lack of pathways to develop skilled analyst. 2/ high false positive rates inundate the few skilled analysts we have
11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?
   Yes, but not how it is commonly understood. We can not have 'cyber skills' first because 'cyber skills' is an intangible combination of skills we generically call cyber skills for ease of conversation. When in reality any single role within cyber itself requires the combination of skills that are not distinctly cyber at all.
   So "Yes" refers to "pathways to cyber security roles" in STEM. We need to graduate specific combinations of skills to fill specific cybersecurity jobs that are lacking today, a business analyst course combined with a software developer would make the perfect generic security analyst BUT a helpdesk/support skilled person who has some business risk theory can be a perfect SOC analyst OR a small business owner who does some cloud certifications can make an ideal CISO for a SaaS. There's no real distinct thing that is cybersecurity skill, but there are a lot of theory that make up the foundations of many, not all, security jobs.
12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?
   It seems straightforward that education of immigration opportunities and accreditation benefits actually are. Excite the target audience to gain their commitments, tell stories about why they should care can be more effective at education than focussing only on STEM.
   An important element not mentioned yet is how professions that are being aged out, phased out, redundant, etc. can provide a valuable pipeline of skills that will be valuable to cybersecurity with minimal retraining.

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?

    No, government should not invest more on streamlining reporting when the scope is so minimal and the challenges have not been identified because reporting at any definition of scale has never existed. First we need to have expanded reporting requirements and evaluate if the current reporting mechanisms are even a challenge that centralisation can address. We simply have a fraction of 1% of what is commonly known incidents actually being reported, there are billions of events that could be reportable incidents every year that go unreported. If even hal;f of what happens get reported it would be an order of magnitude what is considered reportable now. Understanding the problem with data, first requires data to be of statistical relevant amounts of data to actually be collected.
14. What would an effective post-incident review and consequence management model with industry involve?

    Follow the aviation model where applicable, to identify the distinct challenges for cybersecurity
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?

    With government bailouts available and expected, there is going to be many organisations that make risk decisions to be less secure because they expect to be bailed out.

    The best thing government can do is support critical private and public organisations, and limit burdens on the rest through funded investigatory efforts instead of funding recovery which can be a strategic bailout for them. Focus on helping them understand their recovery better, not bail them out by providing them the recovery
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?

    Provide more, smaller, grants that encourage startups to emerge to tackle strategic interests. For example many ideas will be shared in these responses to all numbered questions, there is no reason that government need to deliver them directly and it is in fact feasible to simply provide small grants for startups to emerge to tackle them and develop the needs of government indirectly by government through small investments intentionally excluding big business interest so that innovation can emerge instead
17. How should we approach future proofing for cyber security technologies out to 2030?

    See above, some of these Australian founded startups of today will become the world technology leaders of tomorrow
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?

    These firms are larger than Australia, their interests in Australia are a small part of their business model, and these firms have many many interests and security is a small niche for them. Therefore the firms will never be the same as Australian government interests, they will have a niche within a niche that is aligned to Australian government at best.

    To encourage the Australian cyber security ecosystem, the government needs to expand the CSIRO successes in commercialisation of great ideas that started in government AND in small grants that provide a substantial runway for startups but are too small to attract interest from big firms.
19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

The concept of ‘security by design’ has in practice not proven itself as effective for multiple reasons for software and information technology as it did prove to be effective in areas of technology that are appliance based. Because the software or solution design phase is much later in the production pipeline for non-hardware, adding security in the design phase is too late to be bolted on later. Solution or software design is too late because requirements were established without the necessary security, which then means the initiated project or solution did not know about the security early enough to get the necessary funding or resources for security. When security is considered at design instead of earlier during requirements, the security considerations become things that detail or block progress and that makes the security elements a thing that requires funds and resources be taken from elsewhere OR to add security it is perceived to be added costs. Instead of security by design that causes security as an afterthought and something that must be treated like a compromise that needs to be made - make security part of the requirements so when it comes to the design phase security is already in the budget and security resources are available to the designers.

20. How should government measure its impact in uplifting national cyber resilience?
    How long is a ___ insert the thing you want to measure. If we don’t know it’s a string..
    First define it then metrics can be identified for it. Metrics are coupled to the thin being measured, this question is incomplete and can not be given a more valuable answer without the responder making assumptions about the things that are considered resilience initiatives. And then I could imagine that many pages of assumptions for resilience could be provided too and maybe none are even relevant.
21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?
    Being transparent requires no special responses; you either commit to being transparent and follow through, or you commit to transparency with no intention of it, or you decide transparency commitments are best avoided, What are you being transparent about will be vastly different for each case, for example would you commit to publishing your own footnotes when assessing responses in an act of transparency, or just the parts you decide are going to be adopted into the strategy, or everything in between these extreme opposites? This is another perfect example of an incomplete question that might not gain many useful or any specific responses.