2023-2030 Australian Cyber Security Strategy Discussion Paper

Submissions to the discussion paper close on 15 April 2023.
For further information, email us at auscyberstrategy@homeaffairs.gov.au
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?

- Similarly to how the Government has deployed the 'Cyber Hubs' model on the federal level, shared services are an essential approach to enable smaller organisations, which don't have the resources of larger businesses and can often be a weak link in security, to achieve a reasonable level of cybersecurity. This concept needs to be more broadly deployed at a State level and encouraged and enabled in the private sector. Small and medium-sized businesses are not in a position to invest enough to achieve impactful cybersecurity outcomes. The strategy should support opportunities to pool resources for likeminded organisations to help achieve a better cybersecurity paradigm.
- Additionally, there needs to be a prioritization of security and accountability in the supply chain for critical infrastructure. Original Equipment Manufacturers (OEMs), in particular present a significant risk. While many other sectors have embraced the "shift left" revolution and transformed their approach to security by design, many of our most critical systems and organisations continue to inherit risk from lax security standards and low security maturity of OEMs.

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

- At a holistic level, creating more legislation or regulation is only useful and relevant if it is accompanied by implementation and enforcement. As a reaction to the data breaches last year, legislation was rushed through to increase penalties for privacy breaches from AUD $2.2 million to $50 million. Obviously at this level it is a significant incentive to ensure cyber security is an area of focus for organisations, however, as the previous limit of $2.2 million was never used, there is a question about whether increasing the "limit" actually has an impact. A fine of $1 million that is consistently implemented and enforced – even if that means sending businesses to the wall – would have a much greater impact than a theoretical $50 million fine that isn't substantiated.
- More simply, we believe that existing legislation and regulation should be enforced and used more completely by the regulators before new legislation and regulation is introduced.

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)?

- Using legislative mechanisms to enforce cyber security standards is only viable at a macro level. For example, defining the parameters for the content of standards and enforcement mechanisms, rather than describing in detail the actual standards themselves. Legislation has the potential to date incredibly quickly and as such, is not an appropriate vehicle for detailed standards. This is generally well understood within Government already – for example, with the concept of registered codes in the telecommunications industry, it's supported by overarching legislation that establishes the foundations of such a regime. There would be merit in considering a similar model in the context of cybersecurity, as it is likely that a large range of specific issues will come up over the next 5-10 years, which will need coverage by regulation, but which may need different treatment depending on the industry and / or the potential for more rapid amendment than legislation would allow.

- Consideration should also be given to the model that was established by the most recent tranche of SOCI amendments, where legislation was supported by industry consultation for the establishment of industry-specific standards for risk management, and whether this model has proven sufficiently efficacious, both in terms of engagement levels and the suitability of the obligations that were established to justify its use across the security regulation landscape more broadly.

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?

- Since SOCI has only recently rolled out, it's too soon to see what its impact has been. "Customer data" is always going to be too broad to be meaningful for security legislation; not all data is equal and not all data is important.
- Any inclusion of customer data or systems within SOCI would need to be carefully prescribed, otherwise the potential for virtually every business in Australia to be caught by the legislation would be very real. Over-regulation of businesses in cybersecurity is something that may not be favourable to think about in the current climate of highly publicized data breaches, but it should be part of the consideration as it could potentially lead to a broader 'cooling effect' for the economy.
- A valuable example of effective 'data security' regulation is the Payment Card Industry Data Security Standard (PCI DSS). This standard has been effective through being unusually prescriptive of the controls required, having a thorough and effective audit and control regime (including self-assessment for smaller organizations), and also through having stimulated the creation of a market for services that remove the need for organizations to store the in-scope data (ie, tokenization services). Whether customer data security should be within SOCI, or the Privacy Act, or some new legislative framework, is less important than the need for such legislation/regulation to be comprehensive in its approach to considering the problem.

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

- Company Directors have an obligation to be aware of and support efforts to reduce or mitigate all risks to their business. Ensuring that directors are aware that all risks, including cybersecurity need to be managed, is critical. However, specifically nominating cybersecurity as one that requires special attention is not reasonable. The onus of addressing cyber risk should be on the security and risk experts within organisations to ensure that knock-on effects and linkages of a breach are clearly communicated to company directors. Unfortunately, it remains the case in some organisations that "cyber risk" is interpreted at the senior level as the risk of an executive receiving a spam email or a laptop bluescreening, with the result that cyber risk is sequestered to its own (low priority) corner of the risk matrix. Such attitudes are changing post-2022, but it is still going to be more helpful for directors to think of such breaches in terms of business risk rather than a distinct "cyber risk." It's important to spend time educating company directors on what cyber risk really is from a business viewpoint and ensure there is a focus within the board on cyber risk.
- For certain industries, there may need to be varying levels of focus. For example, CPS 234 has already introduced specific obligations on board members for cybersecurity accountability in APRA-regulated industries. But introducing this as a general obligation for all company directors would appear to be premature at this stage. For some industries, it may be appropriate that accountability for cyber ultimately vest at the executive/board/director level, particularly where

there is a strong nexus between that industry and the security, prosperity, and welfare of the broader nation. In other cases, this may be overkill and simply result in directors focusing their energies/attention on issues related to cyber security at the expense of other non-cyber related issues which are, in their specific role, more important.

2d. Should Australia consider a Cyber Security Act, and what should this include?

- Before introducing a blanket Cyber Security Act, it would be beneficial to start with outlining the gaps and issues. If there is a problem that needs to be solved with legislation, and if it isn't already covered by existing legislation, then let's solve it. A blanket Cyber Security Act doesn't address the bigger issue of the lack of enforcement and application of existing legislation. An industry-government working group to do a needs assessment in this area would be worthwhile.

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?

2i. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?

- The government should not prohibit the payment of ransoms or extortion demands by cyber criminals. As uncomfortable as it is, there are any number of scenarios that could arise where paying the ransom is the 'lesser of two evils' compared to the impact of data loss or system unavailability. That being said, victims of cybercrime would in some cases be better off to have a government mandate that prohibits payments, as it would mean they would not have to make the hard decisions themselves and legitimize their decision making.
- Introducing mandatory information sharing around ransomware payments to enable relevant agencies to improve security and better protect against future attacks is recommended.

2g. 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?

- This should remain a decision for individual businesses, considering all the information and weighing on both sides of the argument. Support from government for that process – e.g. an independent observer to provide experienced input to the process – could be a valuable addition.

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

- At a cybersecurity level, interactions between Governments will only work where there is a high level of existing trust. The implications on sovereignty and national security can easily get in the way of a strong cybersecurity relationship, to the point of nullifying the value of the efforts towards cyber resilience. Being quick to respond to incidents that exceed the capabilities of a regional neighbour is one way to build that relationship. Constant meaningful contact, in the form of relevant security advice and advisories is another. Only when the key Australian Government cyber functions, like ACSC, have those close functional links, will that capability be built in a robust, ongoing manner.

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

- One way to build bridges is by sharing regionally relevant threat intel, and close cooperation between regional CERTs is a key element to achieving that.

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

- Increased transparency is key to better demonstrating and delivering cybersecurity best practices. Given that we all know security through obscurity is not an effective model, there is no reason why government departments should not share significant amounts of their cybersecurity resources with the community.

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

- A majority of the information that needs to be shared will come from industry, so the key question is how to get more information from industry and then share it more broadly. Building trust between government and industry is critical in sharing cyber-related information. Sharing must be two way when possible and there should be the potential for more collaborative efforts between government and industry. Expanding the role of the Joint Cyber Security Centres and the range of services provided would be worthwhile.

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?

- In principle, yes it would improve engagement with organisations that experience a cyber incident. Some organisations will unfortunately likely continue to prioritise saving face rather than customer protection when major breaches occur (notwithstanding the fact that the Privacy Act now contains breach notification requirements, there are a broad range of exceptions and exclusions from this, and it only covers personal information). Such confidentiality may help such organisations engage the ACSC more proactively. In practice though, it may be much harder to balance confidentiality with notification of affected customers. Given that many businesses are still playing catchup, it’s not unreasonable to anticipate more 10 million record-plus breaches in the coming years.

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?

- A broader mandatory reporting obligation *could* potentially improve the available data for understanding the extent that Australian organisations are being targeted by various cybersecurity threats. However, such an obligation would need to be carefully defined and appropriate thresholds set as there would be a lot of ‘noise’ and smaller incidents that would add little additional awareness to a public that is already significantly more aware than it was 5-10 years ago. Additionally, data from any expanded reporting obligation could only feed into one aspect of raising public awareness levels – at some point, constant alarmist messaging starts to wear thin and becomes easy to ignore.

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

- If this is alluding to a model of ISP-level filtering, the use of such an approach for threat blocking can be effective, but this is an area that is prone to expansion of use and misuse and would need to be very closely monitored by an independent third-party agency to ensure it isn’t used for non-threat-related content filtering. That being said, one area where this could be workable would be in DDoS mitigation. This threat, recently seen in the Killnet/AnonymousSudan attacks which originated overseas, could have been mitigated at the internet connections overseas. This would require cooperation between providers at several levels and could only be coordinated by the Australian Government.

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

- While Australia likely doesn't require a tailored approach to uplifting cyber skills beyond its current agenda, we do need to ensure that the Government's broader STEM agenda sufficiently covers the core elements of cyber skills and that it is rolled out to all age groups and demographics.

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

- Government support for expanding capacity and skill levels at the high school and university level is necessary to ensure that we can better meet demand for a cybersecurity-skilled workforce. The inclusion of cybersecurity in non-cybersecurity courses should be a priority. (eg. Teaching security to software engineers, is likely to be more valuable than having an extra spot in a cybersecurity-specific course).
- In the area of accreditation, existing global accreditation schemes already exist and should be leveraged rather than creating additional ones.
- Ensuring that cyber security is a nominated skill on skilled visa migration programs is similarly recommended.

15a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

- Small businesses are often the missing link in the web of creating a better security paradigm throughout the business community. A lack of knowledge and resources create challenges. Grant programs or other forms of government funding or tax credit programs to implement cyber security practices at small businesses would be a positive step, but should learn from the failures of past programs including the Small Business Cyber Security program. Approved education and training programs specifically tailored for small businesses would increase knowledge and awareness and be useful in improving cyber security with small businesses.

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?

- To enhance Australia's cybersecurity technology ecosystem and support the uptake of cybersecurity services, increased funding across a broad range of University and TAFE courses would help move the needle. This doesn't need to be limited to just cybersecurity-specific skills, the industry takes candidates across a wide range of disciplines, often looking more for capability than cyber skills.

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

- It is a fact that it costs more to develop secure systems than it does to develop insecure systems. Therefore, at an economic level, security by design is only going to happen for one of two reasons: (1) the threat/concern of liability for security weaknesses; or (2) market demand. Market demand is certainly increasing, but in many areas, the power imbalance in the market means that software companies do not need to acquiesce to the security demands of smaller customers. If the government enforced security requirements on the technology it purchases, that would be a good start; but enforcing existing trade practices concepts such as "merchantable quality" and "fitness for purpose" to include security would be far more effective.

- Additionally, many basic security design principles (e.g., Open Design) are still yet to fully percolate through to developers of emerging technologies. In particular, the Industrial Internet of Things is an area where vendors continue to rely on security by obscurity and may require further support to understand security by design. Publishing issue-specific guidelines for the major OEMs and establishing basic transparency requirements for the security posture of cloud-enabled industrial technologies would help to ease challenges that are on the horizon (or already here).

20. How should government measure its impact in uplifting national cyber resilience?
    - With the introduction of SOCI reforms and efforts to improve in the wake of last year's data breaches, there is a lot of focus on controls and incident preparedness. However, one other, often underappreciated, area of improvement is attack surface reduction. For example, how many CI orgs are going to find it more straightforward and efficient to simply decommission or modernise or migrate decrepit legacy systems rather than uplift them to meet SOCI requirements? Understanding the magnitude of such decommissioning across CI sectors, and the volume or classification of stored data destroyed, may be one helpful measure of breaches averted through attack surface reduction.