Attachment A: Cyber Security Strategy Discussion – Dr. de Souza-Daw Comments
Paper Questions
This attachment consolidates the questions for consultation in the 2023-2030 Australian Cyber Security Strategy Discussion Paper and includes further specific detail.
Respondents may make a submission regarding the entire discussion paper and full list of questions, or select only those questions which are most relevant.

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?

Education
Minimum Professional Development.
The minimum award for IT staff must include a minimum of professional development. One argue that the minimum professional for IT staff is greater than the minimum hours of professional development for other professions as it changes more frequently and have a wider impact. Similarly, this will help in maintaining currency and qualified professionals.
Suggest: Adding minimum hours of professional development in the Modern Awards under the Fair Work Act.

Transparency
To stop corrupt, weak security practices we need to make sure transparency is available. There really needs to be laws to make sure companies policies/procedures are public or at least accessible to staff and stakeholders.

Criminalise cyber negligence for all directors, executive directors.

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)?

Legislation – only enforces once major damage has been done. Lawyers typically advises clients not to sue unless $50k damages have been done. Hence, small claims are not reported. This could lead to a small incident becoming several more small cases or a major case.

The most important is *transparency.* We (customers/owners) of private data must know how it is used and by whom (e.g. staff positions). *Where, When, What is being stored and why. Legislation of transparent such as relevant policy/procedures should be accessible to all stakeholders at all times is needed. Legislation to keep only data that is needed to do what they needed to do is also required. e.g. Applying for a job should require your personal address. But perhaps at best suburb. Your date of birth should never be recorded but only the year – unless there are policies needing the full date of birth – e.g. day off on your birthday or greater access when you turn 13, 15, 16, 18 years of age, etc.*

Transparency, helps stakeholders defend themselves from cyber attacks and cyber negligence.

Legislate transparency where applicable.

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?

Critical Infrastructure Act – should only apply to the national and state critical infrastructure.
Consider the below example:

A critical electricity asset is:

- a network, system, or interconnector for electricity transmission or distribution for at least 100,000 customers
- a network, system, or interconnector, that transmits or distributes electricity to at least 100,000 customers, or
- an electricity generation station that is critical to ensuring the security and reliability of electricity networks or electricity systems in a state or territory.

It is written clearly and concisely and in conventional risk matrix terms. But what is the asset? The power distribution substation, power generators/station that provides the 100k customers is clearly assets. It does cover "systems" e.g. the software remotely monitoring these sites in an control centre elsewhere.

Seems these definition doesn't consider the customers e.g. a Hospital looses power (critical infrastructure) is that more critical than 100k homes? Or a food supply chain looses transportation abilities due to a shortage of fuel.

I would suggest amending these such that Critical infrastructure assets supplies another critical infrastructure.
e.g.

A critical electricity asset is:

- a network, system, or interconnector for electricity transmission or distribution for at least 100,000 customers
- a network, system, or interconnector, that transmits or distributes electricity to at least 100,000 customers, or
- an electricity generation station that is critical to ensuring the security and reliability of electricity networks or electricity systems in a state or territory.
- A network, system or interconnector that transmits or distributes to another National Critical Infrastructure or Critical Component.

Customer data can easily be written in the same term: e.g.
A critical electricity asset is:

- a lost or stolen data for at least 100,000 customers,
- a data integrity is comprised for at least 100,000 customers
- a data availability is comprised for at least 100,000 customers

There is no reason why customer data can't be considered a *Critical Component to Critical Infrastructure.*

Other Critical components would include minimum trained personnel to investigate, repair, restore functionality, critical spare parts and emergency funds.

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

This is clearly obvious. Any company directors should asset all serious risks including cyber. However, it would also requires then to seek external advice such as security audits on a regular basis. Private schools, governments departments, private industry already do similar audits, e.g. SOC reports, Payment Card Industry Data Security Standard (PCI DSS), etc. Making it compulsory makes non-compliance negligence.
Make cyber negligence a criminal offence for Executive Directors and Directors.

d. Should Australia consider a Cyber Security Act, and what should this include?
Yes, it needs a stronger Cyber Security Act.
Include:
Enforce corporations between government agencies including law enforcement, telecommunication providers and companies. (Please note: data storage and processing such as Cloud providers and ISP are consider telecommunication in this document)
Enforce transparency and communication of the cyber event.
Enforce lessons learned/cyber remedies to the event
Cyber event for neighbouring countries that could or may affect Critical Infrastructure or Critical components of Critical Infrastructure.
Cyber audits of telecommunication, critical infrastructure including encryption, data storage, process and transmit. Security of end-points and security data centres. Most important of the enforcement of other policies/processes that weakens cyber security.
Fines and recovering cost of the investigations/actions.

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 regulator frameworks?

This is a very difficult question. That must be monitored.
One suggestion is to have it as tax deductible with receipt and times. Such that the tax office can give an indication of financial and time consumed.

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?

Laws like this would be very hard to enforce. e.g. Where is the burden of proof how did they collect the evidence? What is worse, Ransomware victims are just that victims, you are effectively making the victim suffer twice.
You are better off blocking (or making it an offence not to block) accounts associated with ransomware, fraud and other financial providers.

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?

Government should always discourage the payment to ransomware actors. Possibly, the fail to report, and the fail to protect e.g. cyber negligence should be a crime.

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

We need to define neighbours – are we talking about what telecommunication links connected to? Or geographic neighbours?
I would argue our Cyber resilience depends more on our cyber neighbours rather than our geographic neighbours. Companies that supply software, encryption, and other ICT products are more critical.

Our geographic neighbours most important is to supply information such as banned IP addresses/websites, known bad software hashes – or we all contributed to the same resource such as virus vault. Educating them on identifying and protecting software/data and vice-versa. We can learn from them.

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

Australia will always have a great need in the following industry:

- Agriculture
- Food Industry
- Transportation
- Telecommunication
- Defence

These are areas we need the best we can. Obviously, cyber applications and security in these areas should be a focus of international 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?

First, focus on protecting Australians with appropriate cyber laws and prosecute cyber negligence.

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

1. Review all policies and procedures to identify how that could cause a cyber incident.
e.g. In practice, demanding staff to reply to emails from unknown sources (typically done to increase customers, generate leds, etc). This can easily encourage phishing emails.
e.g. Using personal phones, computers to access staff emails – easily download Personal Identifiable Information.

These examples are very common in other companies/businesses. This can be done once per an industry and 3-5 years.

2. Microsoft/Redhat and others have in the past all released security manuals for their products. These days such highly details are hard to find and use.

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

Central location of sharing security of end-points. e.g. which group-policies to be blocked/enabled. Which software hashes are safe.
Known threats

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?

There must be an obligation to report. This is the exact opposite of what we need. Government must share information if they believe it will limit or prevent damages to individuals, businesses and governments. Otherwise, the same mistakes will likily to re-occur at the same place or otherwise. Negligent directors and managerial staff often goes on to other places and do the same thing as document by various anti-corruption bodies such as IBAC.

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. But also the ability to prevent ransomware.

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

This is a highly subjective. Obvious machine learning based on user action could be implement on end-points – that forces user intervention would be more scalable than having a centralise server such as splunk/greylog or a SIEM system. Although, these systems would be better are detecting the severity and the breath of the attack.
University research are looking at Artificial Intelligence, questionable how well that would work. Machine learning and predictive behaviour would be better practice.

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

See No. 1 response. Minimum professional development both in time and budget needs to be spent appropriately. This needs to be law.

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

Education – needs professional development to keep ICT staff up-to-date and to develop transfer skills to similar ICT jobs.

Accreditation – Australian Computer Society (ACS) accreditation of degrees and masters are very weak. ICT employers are using online testing sites because they can't tell based on ones transcript even though the higher education provider and ACS both say they are up to a bachelor/masters degree level. There needs to be a major overhaul of Higher Education – this is outside the scope of

this submission. Many employers uses an external testing centre to measure skills of applicants. So why aren't universities using them.

Certification – industry certifications are more appropriate than degrees. e.g. Google https://grow.google/intl/ALL_au/certificates/?tab=career-certificates

Commendation: Government should be commended on their advertisement of reporting, blocking and don't share dubious emails, links and software.

Immigration should be restricted until we have better measure of the persons ICT skills. Creating higher paying jobs should be the focus on keeping qualified ICT staff.

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?

There really needs to be laws on cyber negligence and protection of whistleblowers. Without them, events like Optus/Medicare will keep occurring.

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

Post-incident review:
Owner/Responsible Director(s)
Incident Description
Related Incident (if appropriate)
Policy/Procedures affected/breached
Incident date
Incident duration
Incident response team
Incident responders team leader
Size of the event – downtime, No of customers/staff affected.
Root-cause investigation – must identify appropriate security hygiene, properly equip staff, properly secured devices and whether policy/procedures audits and investigations was actually performed.

Consequence Management
Identify loss and the potential harm. Making sure there are more protection against a "kill-chain" attack. e.g. Identify theft after a phishing email. (You need to intercept the kill-chain), e.g. block ransomware from getting paid through banning financial accounts/blockchain accounts.
Making sure there are sufficient trained staff e.g. to issue new bank cards to protect against identify theft.
Audits of policy/procedures must be done within 3 months and a year and enforce by insurance and government regulator.

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?

Insurance agency – must enforce cyber security audits. Statements on what is the minimum cyber security measure that needs to be enforce for maintaining eligibility for insurance.
Insurance agency – must have plain language statement on what cyber events they insure.
Industry must demonstrate the enforcement of policy/procedures on a regular basis. Please note non-cyber policy/procedure can easily create a cyber incident.

a. Small business – a single website for best practice recommendations and common problems.

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?

Enforce minimum standards. At the moment, we are heavily reliant on due care and due diligence to enforce standards. There should be minimum standards on making sure data at rest is encrypted, access (multi-factor access), transmit/transactions (e.g. blockchain), collection and accuracy of data collected and stored.

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

Minimum security on endpoints, over-the-count purchases or details on how to secure.
Enforce/legislate: The purchases must allow security upgrades for the life of all connected products or turn the connected features off (Connected products: Smart TVs, laptops, fit bits, smart watches, etc).
e.g. a TV may last for 15 years, but only been patches for the last 3 years. After that it is vulnerable.

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?

I would encourage open-source technologies. If Microsoft stops supporting Windows 10 if it thinks it is a pirated copy, then it is vulnerable. So the use of open technologies such as PDF, Operating systems such as Ubuntu, and libreOffice are not susceptible to purchase-prison.

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

Like OH&S, products should be safe to use. Similar, cyber products should be safe to use. Thus, minimum security standards should be enforce. Like Due Care/Due Diligence laws, this needs to be very clear and cyber negligence should be a crime.

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

No. of audits that below minimum standards.
No. of critical security events
No. of known viruses/Bad IP addresses on the network.
No. of cyber insurance payouts
No. of Critical Infrastructure/Critical Components breaches
No. of communications sessions to known bad email/IP addresses/phones.

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

If ideas from a submission is used, then credits on the submission needs to be acknowledged, publicly (for public submissions), e.g. on the website.

Have a draft of the legislation for comments

Have a public timeline of events