Australia Cyber Security Discussion Paper Questions – Responses

[redacted]

Tag Line - KISS – Keep It Simple and Sweet. If this strategy is followed in every aspect, then everyone would be able to follow it correctly. The moment it becomes complicated, people will ignore it.

I. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

Response: I understand from multiple sources of updates that Australia has invested and is investing extensively in below activities to achieve its goals:

- Schools, colleges/universities on Cyber Security education
- Research/development to invent cutting edge technologies for securing Australia infrastructure.
- Cyber Security resources/talents.
- Collaboration with government, Industries, International partnerships to combat cyber threats in Australia and globally.
- Cyber Security Awareness

However, in my perspective Australia should focus on below basic and ground level processes:

i. **A cyber security Gap Assessment** as to where Australia stands today in terms on Cyber Security in Global market. For example, a benchmark survey could prove beneficial. This will help Australia to know how much effort, resources, budget, and time is needed for being the most cyber secure country by 2030.

ii. **Root cause analysis for critical incidents** happened in past 2-3 years that had material impact on Australia's economy. And then to pick required areas of Cyber security and strengthen it.

iii. **To conduct a mandatory assessment followed by trainings for all Australians** and to gauge their knowledge regarding Cyber security, especially to the non-IT people. This would provide understanding of current awareness among the citizens and then the government can arrange basic Cyber security awareness workshops/online trainings to the people to foster their knowledge on the subject. Topic can be more towards, online banking, mobile banking, IOT security, safeguarding their personal data and identity, basic security do's and don'ts with examples of security incidents happened in past in a lay man's language. People participating in such activities can be given goodies to boost them.

iv. **A shift left approach** to be implemented in such way that cyber security is embedded in every aspect of the technology/products like Architectural documents (High Level and Low

level designs), related process, procedures etc. Such document integrated with security controls should be reviewed by security professional. A checkpoint ensuring that all these controls are implemented before the application/server/network device is onboarded in production. For example:

a. If NIST framework is followed then every High level Design document, Low Level Design document, processes, procedures should outline which are the applicable NIST controls for that particular design/process/procedure and how it is implemented. Mapping of the Reference (document section number) to how the applicable control is implemented should be provided.

NIST Control	How it is implemented	Document reference number mapping
800-53 – RA 5 – Vulnerability Scanning	All infrastructure components are added to Qualysguard for performing Vulnerability scanning before the system is moved to production and further on regular intervals.	Document XYZ; section 5 Vulnerability Management
800-53 – AU-2 Audit event	The systems part of the design are integrated with Qradar for SIEM	Document XYZ; section 5 Event Management

b. Likewise, hardening as per standards like Center of Internet Security, encryption, Access Management, Segregation of Duties, secure design and coding, backup, redundancies etc. applicable controls must be verified.
c. It is crucial that any system that needs to go to production shall abide by required security controls implementation and it must have appropriate endorsement for appointed security professional as a part of Security Governance. This could be either for on premise infrastructure or externally hosted infrastructure or cloud hosted infrastructure.
d. Once it is ensured that the newly built system is compliant with all required security controls it should be implemented in production following the Change Management process.
e. There shall be continuous monitoring (like regular cybersecurity audits, assessments, and reviews to identify vulnerabilities, assess risks, and continuously improve cybersecurity measures at national, organizational, and individual levels.) of these systems in production w.r.t required parameters, reporting and remediation in case of any deviation.

v. To achieve all the above there must be strong security governance in place and commitment from the senior management.

II. 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)?

Response: Review of Security Incidents, lessons learned, Risk Assessment and Gap assessment results, Surveys across employees, results of surveys. All these need to be considered in order to mandate appropriate cyber security standards.

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?

Response: Classification policy should be relooked to consider classifying various data types like, personal, health, financial, etc.

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

Response: Yes, senior management plays an important role towards achieving good security posture.

d. 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?

Response: If the organization is aware of security incident they can immediately contain by taking required steps and notify legal and official authorities. In my opinion there would be no impact if ransom is not paid if the organization have appropriate backups. Even by paying ransom no one can assure to get their information back.

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?

Response: Yes it would help organizations/individuals to make them safe behind the Australia law which prohibits paying ransom.

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

Response: Yes, additional measures can be thought of like: scholarship for studying in Cyber security arena, welcoming global talent to fill in the gaps as soon as possible to address resource crunch, embedding Security responsibilities in all individuals activities and integrating it with their performance.

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

Response: While immigration plays a very good role in getting visas globally. Australian government should do audits on skill assessment bodies frequently. I see them disqualifying valid individuals so that the individuals are required to file skill assessment again, in order to gain money. The timeline for skill assessment is quite lengthy e.g., certain skill assessment bodies takes 3 months and even if some experience is not assessed properly by them due to their mistake, they take an additional 3-4 months to correct it. They even take 2-3 weeks to reply to a simple query.

If skill assessment bodies can shorten their timeline and assess the skills fairly then we can get more and more satisfied and skilled workforce willing to come to Australia. I have seen lot of candidates unwilling to proceed due to the challenge in skill assessments.

V. **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?**

Response: There must be a proper Standard Operating Procedure and Knowledge Base kept updated regularly. This will ensure all the incident line 1 and line 2 support would follow right protocol during the incident. Having a single portal would be wise to have for all cyber incidents, as it can be then easily manageable. KISS – Keep it Simple and Sweet.

VI. **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?**

Response: Innovation, New technologies, Industry Best standards like CIS, NIST, ISO27001 etc. Cloud infrastructure Security (to be review by Cloud Governance Forum, proper contract etc.) . Focus on Short term and long-term strategies both. Have a proper planning, roadmap to achieve different milestones.

VII. **<u>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?</u>**

Response: Yes, this will support Australia's economy. Additionally, such firms would be able to deliver cyber security services to support Australia's goal by 2030.

VIII. **<u>How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?</u>**

Response: There should not be any new concept for ensuring security for new technologies. Same onboarding checks/reviews (As mentioned in question I response - Please refer) system to system, technology to technology should be applied even for new technologies. I could think of proper contractual agreement and supplier chain controls in addition to the old ones.

Thank You