Australia’s 2020 Cyber Security Strategy

Monash Submission

1. What threats should Government be focusing on?

Data breaches

From the report of OAIC (https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/), 964 notifiable data breaches are reported in the past 12 months.

6. What customer protections should apply to the security of cyber goods and services?
10. Is the regulatory environment for cyber security appropriate? Why or why not?
12. What needs to be done so that cyber security is ‘built in’ to digital goods and services?

Data encryption should be compulsory compliance for industry sectors with sensitive and private data, e.g., healthcare and finance. Those two sectors are also high-value (top) targets in data breach incidents, as reported in OAIC. Encryption compliance will enforce customer protections and push forward the adoption of ‘built in’ encryption features into digital goods and services. For example, the US Health Insurance Portability and Accountability Act (HIPAA) compliance requires that the health information must be safeguarded via encryption whenever needed.
https://www.hipaaguide.net/hipaa-compliance-guide/

14. How can Australian governments and private entities build a market of high quality cyber security professionals in Australia?

Government should put cyber security profession as the shortage immigration list, across all levels (not just the executive level). Young people with adequate cyber security knowledge (e.g. a master of cyber security degree) should be able to apply for working visa or Australian PR.

20. What funding models should Government explore for any additional protections provided to the community?

The current CRC Cyber Security does not work very well. It is only restricted to a very limited of industries and universities. In order to further widen the scope, the Data 61 model should be adopted and should be further enhanced. Currently Data 61 is working with more than 40 universities across Australia to support their research. More funding from Data 61 should be allocated in the cyber security area, to further allow more universities participate in the research of this challenging area.