Submission in response to "the call for Strengthening Australia's cyber security regulations and incentives"

Disclaimer: The views in this document are solely from an individual perspective and does not represent views of any organization.

I would start off with saying that the very fact that government seeks input from security professionals from around the world is a good initiative and demonstrates focus on cybersecurity. Cyber Security is undeniably the need of the hour. With multiple targeted attacks on individuals, organizations, the need to adapt security practices is an absolute must now.

I have added my views on couple of these items :

How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?

A steering committee needs to be formed if not already present. Board with participation from different industry vertical and leaders is required. Members association from small, medium business required on the steering committee. Policies and regulations are best driven with a top-down approach and forming a committee that represent each business, regulatory, representative ensures that maximum market coverage is achieved.

This committee needs to report to the Federal government.

More awareness campaigns are required targeted towards consumer, individuals and small business . These campaigns should not be technical but informative enough. Each business should also be encouraged to spread awareness to their consumers that way the reach can be maximized.

— Would a cyber security code under the Privacy Act be effective? Why or why not?

It would be effective. A separate code for cyber security in Privacy act will convey the importance on cybersecurity from government perspective. Also, most large to medium organizations tend to comply with privacy laws of countries and hence introducing a separate cyber security code would ensure business will comply with them.

In observation, these are my inputs for the current privacy law:

> The data breach scheme refers to disclosing "Under the Notifiable Data Breaches (NDB) scheme any organization or agency the Privacy Act 1988 covers must notify affected individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved."

It should in my view cover all data breaches irrespective of the current affect known. This would drive business and consumers to put more controls in security. In order to fully understand the current threat landscape, more business/individuals need to report any cybersecurity related incidents. The current statement put emphasis on if the data breach results in "serious harm" however in most cases,

organizations and individuals may not be able to judge the full impact of the breach. All data breaches thus in my view should be disclosed within a provided time frame.

— What technical controls should be included?

Mandatory data usage notice

Providing user Option to opt out of marketing, surveys

Consumer data retention period to be set.

Collecting minimum Personally identifiable information.

Defining time to report a data breach

— Are additional education and awareness raising initiatives for senior business leaders

required? What should this look like?

Yes, educational training around cybersecurity for senior business leaders is essential. I would propose grouping the leaders based on industries purely because while the basic cybersecurity practices remain same, Critical infrastructure, finance require more stringent cyber security controls to be applied. Moreover, the cyber security practices for different industries ensure that best controls are applied to the sector while keeping productivity in mind.

Below approach could be used

Step 1: Inviting influential industry leaders in awareness session and encouraging them to help spread awareness within industry further.

Step 2: Having a webinar for each industry and inviting maximum participants.

In my view this approach would work, as industry leaders can help propagate the practices to a greater reach.

— Would small businesses benefit commercially from a voluntary health check?

Yes they would. In my view small business can use all the help when it comes to cybersecurity as it's not feasible for them to invest in cybersecurity without having any significant returns.

— What other incentives would be required to encourage uptake?

A marker badge to improve customer confidence. These badges should be popularized and could act as a trademark of security in Australia for small to medium business

Publishing list of business that voluntarily comply with standard on gov website

Yearly recognition and award to small business with best cyber security practices

Provide assistance in incident recovery to participating business through a network of voluntary consultants

Providing platform for small business to interact with industry leaders where cybersecurity is in focus.