RESPONSE TO STRENGTHENING AUSTRALIA'S CYBER SECURITY REGULATIONS AND INCENTIVES

DR. PRAVEEN GAURAVARAM

[redacted]

MR. BYRON LANGSLOW

[redacted]

MRS. HARRIET DIANA RICHARDS

[redacted]

TATA CONSULTANCY SERVICES AUSTRALIA

1. What are the factors preventing the adoption of cyber security best practice in Australia? BL We believe that a fundamental skills shortage, a lack of knowledge of the finer ways to implement the essential 8 in small to medium enterprises, and the prohibitive cost to bring in consultants to do this work for home/cottage enterprises.
2. **Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?**

   We believe that an active role from the Government
   (a) in advising the businesses on the right investments in cyber security
   (b) in developing an awareness programme on cyber security incidents, especially in the supply-chains and their social and economic impact
   (c) in amending its regulations with shared responsibility of cyber security for all parties in the supply chain including mandatory notification of cyber breaches by a party in the supply chain
   (d) in benchmarking industry-wide best security practices and promoting security-by-design and privacy-by-design principles both legally and technically through cyber security research and innovation projects in the Universities and simultaneously building the capability and maturity in this industry

   could help businesses from making decisions that are not detrimental to the impacts of negative externalities and information asymmetries.

3. **What are the strengths and limitations of Australia's current regulatory framework for cyber security?**

   Australia's current regulatory frameworks of Privacy Act 2008, Australian Consumer Law and Corporations 2001 appear to be working well when applied to cyber security even though they were not originally intended for cyber security and had their share of limitations as observed in the discussion paper. However, in view of prolific advances in cyber-attacks and their ever-changing nature and scale, we may see a need in addressing regulatory limits specifically targeted for the loss of cyber-attacks including Denial of Service on business operations, digital extortion attacks such as ransomware attacks, email forgery, and legal fee associated with the investigation of breaches[1]. The cyber insurance is generally covered by the laws, some of them had been there well before the advent of Internet such as the Insurance Act 1973 and the Insurance Contracts Act 1984 and the Corporations Act 2001 and the common law.

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

   Australia's regulatory environment has changed over the years to encompass such safety devices in the Automotive Industry such as mandatory seatbelts, airbags, and safety ratings. Through a concerted effort from government in consultancy with the private sector, and through mediums such as these consultative processes, the Government can mandate the requirements to safely operate ICT, and educate all Australians in the same manner that every Employee understands OH&S. Through a series of necessary trainings (such as driver education, but in cyber security awareness) that must be undertaken and assessed every year to enable the citizen to understand the basics of Cyber Security, Phishing attacks, and how to be aware of scam calls etc. These can be computer based trainings, provided by service providers across Australia, which when the tests are passed, will update a central license location, recording that the individual/employee/business has a basic understanding of Cyber Security, and

[1] https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/australia

this could help reduce the instance of Ransomware infections, people being taken by scams, and visiting or interacting with shady websites and online portals.

5. **What is the best approach to strengthening corporate governance of cyber security risk? Why?**
6. **What cyber security support, if any, should be provided to directors of small and medium companies?**
7. **Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?**

The best approach to strengthening corporate governance of cyber security risk is driven by several factors including the social & economic impact of a cyber-attack on an industry, return-of-investments for the enterprises from complying with the mandatory standards and regulations and the practical viability of such standards and regulations and their impact on business supply chains. We believe that voluntary governance standard is the most practical approach for strengthening corporate governance of cyber security risk with mandatory governance standard as a placeholder for the enterprises to comply with, in the event of a serious cyber security incident or failure to implementing adequate cyber security practices, for a reasonable period before moving the requirements to voluntary governance standard.

When to comes to small and medium companies, the University sector could be leveraged in providing security consulting and advice on adequate security measures that these companies need to practice and thorough testing of these practices through students' projects.

Cyber security awareness among senior business leaders in the organisations has been developing. However, it is helpful for the executives to be aware of cyber security metrics in their organisations and supply chains that influence their business decisions. For example, this could be in the form of real-time executive level dashboards with the right strategic, tactical, and operational metrics relevant for their business and industry which can be looked upon to make cyber security dependent business decisions.

Chapter 5: Minimum standards for personal information

Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?

What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?

What technologies, sectors or types of data should be covered by a code under the Privacy Act to achieve the best cyber security outcomes?

Chapter 6: Standards for smart devices

What is the best approach to strengthening the cyber security of smart devices in Australia? Why?

Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt for as a standard for smart devices?

a. If yes, should only the top 3 requirements be mandated, or is a higher standard of security appropriate?

b. If not, what standard should be considered?

[For online marketplaces] Would you be willing to voluntarily remove smart products from your marketplace that do not comply with a security standard?

What would the costs of a mandatory standard for smart devices be for consumers, manufacturers, retailers, wholesalers and online marketplaces? Are they different from the international data presented in this paper?

Is a standard for smart devices likely to have unintended consequences on the Australian market? Are they different from the international data presented in this paper?

Chapter 7: Labelling for smart devices

What is the best approach to encouraging consumers to purchase secure smart devices? Why?

Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?

Is there likely to be sufficient industry uptake of a voluntary label for smart devices? Why or why not?

a. If so, which existing labelling scheme should Australia seek to follow?

Would a security expiry date label be most appropriate for a mandatory labelling scheme for smart devices? Why or why not?

Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?

Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?

Chapter 8: Responsible disclosure policies

Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?

Chapter 9: Health checks for small businesses

Would a cyber security health check program improve Australia's cyber security? If not, what other approach could be taken to improve supply chain management for small businesses?

Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?

If there anything else we should consider in the design of a health check program?

Chapter 10: Clear legal remedies for consumers

What issues have arisen to demonstrate any gaps in the Australian Consumer Law in terms of its application to digital products and cyber security risk?

Are the reforms already being considered to protect consumers online through the Privacy Act 1988 and the Australian Consumer Law sufficient for cyber security? What other action should the Government consider, if any?

Chapter 11: Other issues

What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights consumers?