STRENGTHENING AUSTRALIA'S CYBER SECURITY REGULATIONS AND INCENTIVES

SUBMISSION TO

DEPARTMENT OF HOMEAFFAIRS

BY PRASHANT SINGH

[redacted]

GOVERNANCE STANDARDS FOR LARGE BUSINESSES

What is the best approach to strengthening corporate governance of cyber security risk? Why?

- Cyber security should be embedded into the business processes at every level , similar to OSH standards
- Corporate Board should be held liable for serious cyber security breaches and there has to a measurable KPI against this measure in annual reporting.
- Cyber Security awareness training should be made mandatory for every corporate board member
- There will be initial cost associated with raising awareness and education amongst the business ,cost which will be offset by reduce Cyber Security risk

GOVERNANCE STANDARDS FOR LARGE BUSINESSES

Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?

- As per most IT survey done, most senior business leaders lack basis understanding of Cyber Security and its associated risk
- Cyber Security awareness training should be made mandatory for every senior business leader and board members
- Training should be made available Online with Digital Certificate issued upon completion with an expiry date .This can be administered via existing registered training organisation (RTO)
- Cyber Security training for senior business leaders will assist in Australia transform in Digital Business by 2030.

MINIMUM STANDARDS FOR PERSONAL INFORMATION

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

- Cyber Security code should sit outside Privacy Act and supplement it as the Privacy Act does not apply to lost of small business

What technical controls should be included?

- Personal information should be Encrypted In Transit and Encrypted At Rest
- Media Sanitation and Disposal Policy developed
- Secure configuration of hardware, storage, operating systems, databases, middleware, and applications

What technologies, sectors or types of data should be included?

- Cyber Security code should apply to business, including Non for Profits , Charity and Community Organisation dealing with customer data .
- It should apply to all sectors should practise Basis Cyber Security Hygiene when dealing with Personal Information
- Health Data, Financial Information, Personal Information, Banking , Insurance etc

MANDATORY PRODUCT STANDARD FOR SMART DEVICES

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

- Every device should have Cyber Security ratings and recommended best practice just like User Guide included in the packaging.

If so, should we adopt internationally recognised standards (ESTI EN 303 645)?

- Cyber security provisions for consumer IoT should be adopted

What would be the costs?

- Cost should be part of manufacturing and selling Cyber safe product , similar to Electrical safety or Child Seat safety standards

Would there be unintended consequences on the Australian market?

- Yes, I can only foresee increased sales of Cyber Safe devices on back of increased consumer confidence .

LABELLING FOR SMART DEVICES

Is a label for smart devices the best approach to encouraging consumers to purchase secure smart devices? If so, should it be voluntary or mandatory?

- Cyber Security Start Rating label as same as car security rating . This should be mandatory of every Smart Devices.

Would a combination of labelling and standards be effective?

- This will increase Cyber Security awareness for consumer when buying Smart Devices

Should mobile phones be included?

- Yes

Should the label be digital and physical?

- QR Code based Digital label
- Star Rating to be display on packing

RESPONSIBLE DISCLOSURE POLICIES

Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? Why or why not?

- Voluntary disclosure should be adopted by every companies dealing in Technology.
- Secure channels should be provided to that allows security researchers to safely report found vulnerabilities
- This will increase the overall Cyber Security posture and reduce risk.

VOLUNTARY HEALTH CHECK FOR SMALL BUSINESSES

What is the best approach to strengthening supply chain security for small businesses?

- Cyber Security awareness training should be made mandatory for every small businesses at every level of supply chain who deal with customer data
- Cyber Security Centre of Expertise should be made available to all Small businesses.
- Basis Online Cyber Security Awareness training should be part of getting an ABN /ACN

VOLUNTARY HEALTH CHECK FOR SMALL BUSINESSES

Would small businesses benefit commercially from a voluntary health check?

- Small business will benefit commercially from a voluntary health checks.
- Getting a Cyber Security Compliance tick will increase business customer value
- This will increase confidence of customer using those services.

VOLUNTARY HEALTH CHECK FOR SMALL BUSINESSES

What other incentives would be required to encourage uptake?

- Cyber Security Health checks should be offered to all small Business .
- Create regional and local Cyber Security Centre of Excellence" at existing TAFE & Universities or regional business centres. This will increase Cyber security skills and provide new jobs
- Cyber Security Health Check & Training Credit should be made available to every small business to procure those service from participating "Centre of Excellence".
- Cyber Security Training Credit should be for the basis, refresher and advance industry specific program and should be an on going activity as part of business renewals

CLEAR LEGAL REMEDIES FOR CONSUMERS

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

- The ACL terms should be made more simpler and made more inclusive for consumers.

Are the reforms already being considered to the ACL and Privacy Act to protect consumers online sufficient for cyber security?

- This should be reformed and strengthen further

THANK YOU

"5G, AI, Starlink and other new technologies will create our future industries . Cyber Security fundamentals we put in place today will help create our digital future .COVID-19 pandemic has increased our reliance on Digital Technologies in every aspects of our life . Cyber Security reforms has potential to create new jobs, future jobs and cost we pay now will be offset by reduce cyber risk , creation of new future industries and help transform Australia into Digital Business age. "

– Prashant Singh , Perth Australia

[redacted]

[redacted]