SUBMISSION TO THE DEPARTMENT OF HOME AFFAIRS FOR AUSTRALIA'S 2020 CYBER SECURITY STRATEGY

Sirviro Ripepi - November 2019

The internet is an integral part of society used for endless possibilities and opportunities. Societies' digital presence and identity is growing at an immeasurable rate and inevitably open to vulnerabilities and risks that the average person is unaware of. A national cyber security strategy is the Government's playbook for protecting the Australian public's online activities and indirect consequential suffering to daily lives away from the internet. The Australian public expect the Government to defend their online presence from cyber-attacks in the same way the Government defends the public's safety on the streets. Australia is highly capable to be a world leader in cyber security to fortify the digital ecosystem that spans globally.

Below are four practical actions that Australia can consider to strengthen their position in the field of cyber security: -

1. **Amendment of The Assistance and Access Bill 2018**
   The Assistance and Access Bill 2018 concerns tabled from submissions sought in October 2018 needs to be amended as a key priority so that it complements the Australian 2020 Cyber Security Strategy. The bill presently undermines all defensive efforts of the cyber security strategy in its current form and conflicts with Australia's obligations of the EU's General Data Protection Regulation (GDPR) as published on the Office of the Australian Information Commissioner's website.[1] The Australian Institute of Criminology published a report in 2018 estimating economic impact of identity theft of $2.65 billion.[2] It is imperative to build indecipherable encryption into online systems to help bring secure Australian technologies to the market rather than weaken the technologies as described in the aforementioned bill.

2. **Introduction of a national digital identity certificate**
   Introduction of a national digital identity certificate based on elliptic-curve cryptography will pave the way for a secure and resilient cyber activity. A trusted Australian Government supplied digital identity would increase the security level for all residents of Australia. The digital identity can be used as proof of identification for signing contracts, securely applying for services online such as banking, used for secure future national internet voting and an alternate to a handwritten signature. This would also be a mechanism for combating identity fraud, tax fraud, bank fraud, credit card fraud, etc. Approximately 23 countries have implemented digital identities with the public of Estonia recognised as the leaders for embracing and benefiting from the technology. It is worth researching and leveraging off the good work already done.

[1] https://www.oaic.gov.au/privacy/guidance-and-advice/australian-entities-and-the-eu-general-data-protection-regulation/

[2] https://www.aic.gov.au/publications/rr/rr15

3. **Legalising core online privacy rights similar to GDPR**
   The redevelopment of the Australian 2020 Cyber Security Strategy should consider adapting other influencing legislations to strengthen the outcome of the strategy. In particular the Privacy Act 1988 brings little bearing for accountability and is not flexible enough to be relevant for emerging and disruptive technologies. Technology giants born outside of Australia are pushing their boundaries by obtaining and selling individuals data without consent to the detriment of public safety. The EU GDPR has come about because of the internet and gives Europeans power of their own data. The Privacy Act 1988 should be amended to incorporate the eight Rights as written in the EU GDPR as a minimum which will in turn help Australian businesses comply more effortlessly with the EU GDPR. At present Europeans living in Australia have more rights than Australians which does not make sense. Everyone should have equal rights in Australia. All States and Territories should be encouraged to align the same principles in their regions Privacy legislations.

4. **Including cyber literacy in primary school syllabus**
   Data has been described as the most valuable resource in the world, far more valuable than natural resources like oil and gas. To become global leaders, our future generations need to be educated on basic cyber security principles and rights from an early age, which underpin and govern data as a profitable resource. The internet of things is adopted by youth from an early age with no understanding of the impact to their digital footprint and privacy of their information that is recorded in the cloud for the rest of their lives. The problem lies in the fact that these children cannot look to their parents for guidance as the average parent has low awareness of digital risks, due to late exposure to new technologies. Youth are our future leaders and protectors of this country and therefore should be educated at an early age to shift the thinking of what privacy means for this generation and impacts for our digital future.

   Cyber security is a gateway topic which can bridge and excite children into professions of the future since it touches upon various areas such as artificial intelligence, process mapping, using innovation and creative thinking to tackle everyday problems, mathematics, and more. Infusing every Australian with this knowledge will transform and evolve every future worker and industry in Australia to have a high baseline knowledge of cyber literacy. This will ensure our responsiveness to cyber security issues as a community improves to reduce potential damage. Strong community action can help to avoid the establishment of poor data-protection precedents at industry level being set due to inaction, that then take too long to remedy. It will address issues that we have experienced in the past such as: law-making being too slow to keep up with the impact of new technologies; and known problems related to privacy breaches, taking too long to become actionable and newsworthy in the mainstream media. With artificial intelligence being built-into more everyday products and industries, we need to prepare our future workforce with people who can challenge, lead and pioneer technology in a way that is ethical and protective of both social and economic data interests.

I hope the views presented will be taken seriously and adopted to protect Australia, individuals, businesses and our economy.