Australia's 2020 Cyber Security Strategy - Submission

Name:	Craig Templeton Robert Cumming
Title:	Chief Information Security Officer Information Security Manager
Organisation:	REA Group
Email:	[redacted]

Q01 What is your view of the cyber threat environment?

- The barrier to entry for cybercrime is low, but impact of attacks is high
- Businesses (outside of the ASX 20) are more reactive than proactive.
- The Notifiable Data Breach scheme has had its intended effect - increasing the visibility of the problem (to government) but there's still uncertainty in the next steps and whether or not more legislation is required (or if this will even address the problem).
- The commoditisation of cyber weapons is problematic for smaller organisations.

Q01 What threats should Government be focusing on?

- Cyber literacy - it needs to be part of the vernacular and a baseline security awareness should exist for all Australians, in the way that the TAC's awareness campaigns are for driver safety.
- Small business (90% of the economy) particularly, have low cyber literacy, and are finding themselves more and more targets as part of the supply chain.
- Supply chain risk - increased focus on the whole of eco-system is essential instead of only "critical infrastructure". Attackers will simply pivot to the weakest link.
- IoT - there is little regulation in an industry riddled with security bugs.

Q02 Do you agree with our understanding of who is responsible for managing cyber risks in the economy?

- To some degree yes, we believe vendors, owners of infrastructure should be leaders and not rely on end-users to protect themselves since they have limited ability to do so.
- However, if we don't educate people to understand simple steps they can take to protect themselves (in the same way you're told to slip-slop-slap and wear a hat in the sun to avoid sunburn) they will fall into the trap of thinking that the government will protect them, and no action is required. So, we believe there is a need to focus on a peer-to-peer not parent-child relationship with the Australian people.

Q03 Do you think the way these responsibilities are currently allocated is right? What changes should we consider?

- Public Sector view: Although a number of cyber authorities have been consolidated - there is likely more of this required within federal and state governments in order to streamline accountabilities and resources.
- Private Sector view: Organisations (particularly ASX 100) are better equipped to understand that cyber *is* a risk, however the issue typically lies to how this is then delegated internally. There's typically a scenario where a CISO is "accountable" for a "cyber risk" which results in poor risk management. Where a CEO is "accountable" and business stakeholders are "responsible" for mitigating cyber risk, there are typically better security outcomes.
- Does not appear that we've considered the role of local government (councils) in the strategic view, who manage or maintain critical infrastructure services.

Q04 What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?

- Government should provide more assistance to the Health sector, as the levels of cyber literacy are low and investment in IT infrastructure appears to be poor (consider recent ransomware attacks). Front line service resource allocation suggest this sector does not prioritise basic cyber hygiene despite being the custodian of highly sensitive information.
- Use methods such as the JCSCs to share industry-specific intel that may help CEOs or CISOs better align their strategies to real-world threats.

Q05 How can Government maintain trust from the Australian community when using its cyber security capabilities?

- The government needs to hold itself to the same level of account as the private sector. Government departments should not be exempt from any reporting regimes.
- Cyber literacy of government staffers should be improved. Ministers (and their assistants) should receive a level of training so they can have (at least basic) conversations with their department executive teams on how they are managing cyber risk, in the same way a board of directors may discuss cyber with their CEO or risk committees.
- The government needs to craft a good story where the areas of personal privacy are conceded for the greater good. This may include areas such as encryption legislation, information sharing (across non-cyber related departments) and the introduction legislation that may not have the correct checks and balances. Although the security community may understand why this is needed, the general community are sceptical of these motives.

Q06 What customer protections should apply to the security of cyber goods and services?

- The same protections that apply to retail goods. If a security company claims their product can do something, it should adequately perform that security service. If it doesn't, the customer should be able to return it for a refund. Security vendors tend to over promise and under deliver, how do we ensure they are meeting the needs of their customers?
- Security vendors should not demand payment for remediating code defects and vulnerabilities.
- Vendors of devices that are expected to last 2/5/10 years (e.g. fridges, microwaves, thermostats, TVs etc.) should be required to support the device as long as the ACCC deems is an acceptable timeframe for it last (e.g. a fridge that lasts for 10 years should receive updates for 10 years).
- When internet connected devices are end of life (and are no longer supported) they "default to secure" by disabling their "smart" abilities.

Q07 What role can Government and industry play in supporting the cyber security of consumers?

- A large-scale awareness campaign focused on cyber safety and trust (In the same vein as WorkSafe, TAC etc.)
- Creating forums for small/medium business to interact with larger (more mature) organisations to help them build their cyber resilience programs.
- Additional Government funding for IDcare will help all Australian's who are subject to identity theft.
- The Government should consider mandating 2FA (two-factor-authentication) for any internet-facing service protecting personal information. This would significantly change the economic effort required to commit cyber crime.

Q08 How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?

- Minimum standard for IoT devices entering Australia. How do customers even know when their device is end of life and no longer receiving security updates? (Or how do they even know it needs security updates?)

Q09 Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?

- Conferences - the government should participate in and sponsor but not deliver conferences (such as the recently successful Cyber Con 2019 in collaboration between ACSC and AISA.)

Q10 Is the regulatory environment for cyber security appropriate? Why or why not?

- Regulation could be improved in areas where maturity is low (e.g. industrial control systems, smart health, consumer IoT, consumer routing products).
- The challenge is the speed of change, where almost any device (e.g. kid's toys) could have a network device, wireless receiver, microphone or camera in it.

Q11 What specific market incentives or regulatory changes should Government consider?

- IoT - consumer device minimum standards.
- Health - consumer and commercial (hospital grade) offerings having minimum in-built security mechanisms so that when they are end of life, they default to secure.
- Medical equipment suppliers should be compelled to support basic operating system patching and upgrades that do not cause failures in the equipment.

Q12 What needs to be done so that cyber security is 'built in' to digital goods and services?

- We believe this area requires legislation unfortunately, because voluntary codes are falling short of providing any sort of costumer protection.
- Manufacturers should be required to ensure their products can be updated to patch security vulnerabilities.
- The reuse of default passwords across an entire product line should be discouraged.

Q13 How could we approach instilling better trust in ICT supply chains?

- Mandatory security controls that are known to be effective. Such as (but not limited to) multi-factor authentication.
- Repeat offenders (particular bigger managed service providers) don't suffer any real consequence for privacy breaches. E.g. California publicly disclose privacy breaches - where companies rely on reputation, this could provide incentive to priorities security of the organisation over other priorities.

Q14 How can Australian governments and private entities build a market of high-quality cyber security professionals in Australia?

- Quality of teaching - difficult for the education sector to attract high-skilled professions due to skill shortage (and higher remuneration) in the private sector.
- Create entry level positions within government agencies to build capability. Partner with universities to create 'sandwich courses' where students receive real world experience and companies benefit from additional headcount.
- Create incentives for small/medium business to hire and train cyber security staff, e.g. through the tax system
- Don't reinvent the wheel – look at what other countries have done in this area.

Q15 Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?

- Threat attribution is putting the value of cyber insurance at risk if the policy clause for "act of war" clause is invoked following a cyber incident, e.g. after NotPetya, Zurich insurance refused to pay cyber insurance claims based on attribution;
- ref: https://www.itgovernance.co.uk/blog/an-act-of-war-zurich-american-refuses-to-pay-out-on-cyber-insurance-policy-following-notpetya-attack
- Cyber attribution is not helpful to business and should be kept for Government information purposes.
- Understanding what value cyber insurance actually gives a business - lack of consistency amongst policies.
- Understanding what businesses need to do in order to comply with their cyber insurance. I.e. if I don't have X thing, does that mean my insurance is void?

Q16 How can high-volume, low-sophistication malicious activity targeting Australia be reduced?

- Australia is not a big country and therefore it is likely that someone could DDoS the nation; do we have adequate mechanisms to prevent this? To prevent a large-scale attack against Australia?
- Border-routers could prevent the most basic attacks from occurring at least for the public sector
- Australia should learn from the work conducted by the NCSC in the UK in this area.

Q17 What changes can Government make to create a hostile environment for malicious cyber actors?

- The term "hostile environment" is not helpful. The Government should raise the economic costs of an attack by raising the bar across the board. E.g. stronger controls preventing malicious number porting, mandatory 2FA,
- A high level of cyber-hygiene would be a cost-effective approach; however, this does not mean mandating ASD essential 8. Application whitelisting for example, is expensive, disruptive and hard to implement in the private sector regardless of its theoretical benefits.
- It would be beneficial for the teams writing standards to understand corporate IT challenges since many recommendations are impractical to implement.

Q18 How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?

- Knowledge sharing forums, the issue being is how to better disseminate this information to smaller businesses that is actionable.
- Understanding how many small / medium businesses are actively engaged in services such as stay smart online - how do we know if our messages are getting through?

Q19 What private networks should be considered critical systems that need stronger cyber defences?

- Primary services that would result in harm or state-wide disruption (not limited to):
  - Power
  - Water
  - Waste Disposal
  - Sewerage
  - Fuel
  - Airports & Ports
  - Transport (I.e. Traffic Management / Public Transport)
  - Heath Services (Hospitals and associated infrastructure)

Q20 What funding models should Government explore for any additional protections provided to the community?

- University and TAFE funding of cyber courses should be linked to realised job outcomes. I.e. there is no point having poorly trained cyber professionals with no links to industry and/or jobs.
- Subsidising entry-level roles within the public sector to allow for recruitment in government organisations that would struggle to compete with the private sector for talent.

Q21 What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?

- Lack of security professionals with the correct clearance levels. Pathway for security professionals who are not working in the public sector, to receive levels of clearance commensurate with information they need to receive to inform their organisations of risk.

Q22 To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?

- Strongly agree - general cyber literacy is low.
- As mentioned earlier, there is a great opportunity in this space. We may also learn from other sectors such as road safety or health. Behaviour change is not unique to online safety.

Q23 How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?

- In the same way safety in the workplace has become a water-cooler conversation, we want cyber to be spoken about in the same way.
- We also want consumers to be incentivised to find the "most secure" products and review accordingly, in the same way they would with a product they are delighted by.

Q24 What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?

- Telstra and REA Group ran an extremely powerful (internal) series called CLASSIFIED - this was a series of cyber security awareness videos with the quality of a mini TV series.
- Security Influence & Trust Group (https://sitempowers.com/) has collaborated with StaySmartOnline on several public awareness campaigns.
- TAC's Towards Zero (and associated campaigns)
- WorkSafe and Workcover campaigns.

Q25 Would you like to see cyber security features prioritised in products and services?

- To some degree - it would have to be clear cut and live with the consumer for the life of the product.
- I.e. when someone purchases a tv with a 5-star energy rating, they probably forget about it once they take the sticker off. How do they ensure that once the product is out of security support they are reminded to renew or replace it?

Q26 Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?

- There is a real disconnect between TAFEs and University cyber degrees and job outcomes. We would like to see learning institutions reporting on how many students are being employed as a result of their course completion rates.
- Cyber safety should be viewed as a digital life skill.