RESPONSE TO AUSTRALIAN GOVERNMENT CYBER SECURITY STRATEGY 2020.

DR. PRAVEEN GAURAVARAM

[redacted]

MR. BYRON LANGSLOW

[redacted]

TATA CONSULTANCY SERVICES AUSTRALIA

1. ***What is your view of the cyber threat environment? What threats should Government be focusing on?***

In Australia (unlike USA, UK[1] for example) we don't seem to have a regulatory framework and standard recommendations for Industrial Control Systems (ICS) and Operational Technology (OT) security. ICS and OT environments are vulnerable to both the weaknesses originating in the IT Infrastructure as well as those of their own. While Research & Innovation and cyber security practices are reasonably matured in the arena of IT infrastructure, which cannot be said for ICS and OT security. It is also not sure if the Government has sufficient visibility in the threat environments of Australian critical infrastructure industry including Utilities, Transport, Oil & Gas, Mining and Energy & Resources to be able to develop a national regulatory framework and recommendations. Hence, Government should focus on developing a framework for policy development and long-term view for regulatory framework and business continuity focusing on both IT and ICS & OT security. This means the Government should focus not only on threats on IT systems such as different forms of Phishing, Malware and Web-based attacks but also those specific on ICS and OT systems such as flooding & Denial of Service (DoS) attacks, Man-In-The-Middle (MITM) attacks between Human Machine Interface (HMI) and devices in an OT environment.

This gap presents an opportunity for some of Government investments such as Cyber Security Cooperative Research Centre (CSCRC) to engage in OT and ICS cyber security research and innovation and make a recommendation during the course of CSCRC to the Government to formulate a regulatory framework and policy development.

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

Our understanding of shared responsibility of cyber security is not complete. While the responsibility has to be shared among the businesses, it is also necessary for Government to be a trusted source for private industry in cyber security matters.

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

[1] http://blog.wallix.com/industrial-control-systems-security-ics

Currently, the way responsibilities are allocated is not right as Government has a very limited role in being the right entity to speak on behalf of Australian industry and public in cyber relevant matters. Being a prime representative of Australia and its social and economic state, Government should have more responsibility than anyone else in cyber security as a trusted entity for all businesses operating in and out of Australia with interests in Australia. Relevant representatives of industries and specific companies of these industries should be made responsible for cyber security. These representatives should collaborate and jointly report to Government in an honest and transparent manner on their cyber security capability, awareness and posture on a regular basis. Government's role as a trusted partner in cyber security is the key to enable this conversation between the Government and Industry. This will also promote Australia as a nation which is serious about cyber security of all companies doing operations in the country and hence will attract foreign investors.

Also, although Australian parliament passed Mandatory Data Breach laws for organisations/ industries regulated by Australian Privacy Act it is unclear if all organisations strictly adhere to the Privacy Act or even showcase their compliance with the Privacy Act.

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

There appears to be a huge gap between the way the Government addresses the most serious threats to the way government agencies and private institutions do in Australia: Australian Cyber Security Centre leads the Government's operational response to cyber security incidents. But when it comes to businesses and institutions in Australia, its role is limited to being a hub for collaboration and information sharing. While current legal system does not permit Government to proactively identify systems that are vulnerable to serious threats, Government can still demonstrate its thought leadership in cyber security proactively. In this respect, Government should be a proactive messenger of latest security threats and update the businesses and institutions towards identifying these threats and ways to protect against such threats. Perhaps through its Joint Cyber Security Centres, Government can offer a one-to-one communication set up to the interested businesses and institutions in such a way that the Security Operations Centres of these businesses can collect information feeds on latest threats round the clock from the Joint Cyber Security Centres. This might still be within current legal framework and complements current offerings of Australian Cyber Security Centre to the businesses and institutions.

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

Maintaining transparency in Government communications and privacy of the individuals, businesses and institutions are critical for Government to have a continued trust from the Australian community.

6. ***What customer protections should apply to the security of cyber goods and services?***

7. ***What role can Government and industry play in supporting the cyber security of consumers?***

The best support Government and industry could provide supporting the cyber security of consumers is by improving their cyber awareness through appropriate channels. For example, a bank or a retailer should educate customers to beware about fake offers and calls received from fraudsters via customer-registered communication channels such as e-mail. In addition, these industries could set up cyber awareness booths in their branches to encourage customers know what to do/what not to do when it comes to using personal computers and devices and bank/retail resources. Similarly, government agencies can help Australian consumers of their services on several cyber awareness programmes.

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

For both Government and Industry one of the big challenges is to have a proper assurance on the security and IT technologies offered by the third party IT & Security Services vendors. These technologies often include those of these vendors' and their partners including products and services from start-up and SME enterprises. Both the Government and Industry do not seem to have enough visibility and assurance on the security of these products and services and often the service level agreements push the liability towards the customers (i.e Government and industry and their customers).

One way to improve this situation is to have a common infrastructure where products and services, especially new technologies and untested methodologies, can be tested out for any vulnerabilities and threats. This infrastructure is called cyber range. Right now, cyber ranges in Australia appear to operate in silos, for example, in research institutes, government agencies and industries (telecom, banking, utilities etc.) but is not in a federated capacity by connecting various individual capacities so that cyber attacks and hence security measures can be addressed in a holistic way.

Also, through Federated cyber ranges, the Government can give an opportunity for start-ups to use this infrastructure to validate their security technologies against diverse industry requirements/standards, cyber attacks and hence significantly contribute to the cyber Innovation.

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

It is highly recommended that Government and private sector do not delegate cyber security related functions to one another. Rather, they can work together towards establishing joint infrastructures and work in partnership to improve Australian cyber security capability.

10. ***Is the regulatory environment for cyber security appropriate? Why or why not?***

The current regulatory environment for cyber security does not seem to be appropriate. Some reasons include:

- It is unclear whether Government and regulatory authorities have even decent awareness on the security and privacy risk posture of various organisations[2] in Australia as these companies are permitted to only voluntarily share information related to an incident or potential incidents with a regulatory authority subject to the restrictions in the Applicable Laws such as the Privacy Act.

  Note that the regulatory requirement of Mandatory Data Breach Notification (or Notifiable Data Breach Scheme) poses an obligation to organisations to notify The Office of the Australian Information Commissioner (OAIC) and affected individuals about the information on breaches and contacts of the organisation that got breached is very much an after-thought and does not really help to proactively communicate to the Government and regulators on the security and privacy posture of organisations.
- There are currently no 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[3]. 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.
- As noted in response to (1.), there are currently no regulatory frameworks for the risks in the operational technology industry which is prone to huge cyber security threats.

11. What specific market incentives or regulatory changes should Government consider?

Market Incentives: Government should encourage multi-national companies with strong presence in Australia, by providing them with tax incentives, to open Research & Innovation Labs focusing on cyber security and adjacent domains meeting the needs of Australian market and contributing to cyber security industry growth. It also provides an opportunity for the Government to capitalise on the global innovation capabilities of these companies that can significantly foster Australia's innovation footprint.

Regulatory Changes:

Refer to responses to (1.) And (10.) that demonstrate the aspects where there is a need for regulatory changes.

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

[2] https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/
[3] https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/australia

At first we need to focus on building essential cyber security into digital goods and services. For example, implementing security strategies such as ASD eight essential mitigating strategies into the digital goods and services[4] can be seen as the initial step. Federated Cyber range test beds discussed in (8) are highly relevant to test the products against sophisticated attacks and subsequently the baseline implementation strategy need to be expanded to address any sophisticated attacks discovered.

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

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

This is possible by inculcating cyber security awareness and skills into the roots of our educational system. High school curriculum should include courses and exams on cyber security and Universities should include it as a specific discipline amended to Information Technology or Computer Science undergraduate programmes. Government and Corporates should encourage these students to take up internships and work with them on real world projects in various facets of cyber security.

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

- As noted in (10), there are currently no 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. The cyber insurance is generally covered by the laws that came to existence before the advent of wide adoption of Internet (such as the Insurance Act 1973 and the Insurance Contracts Act 1984) and other laws including Corporations Act 2001 and the common law.

  It is important to develop a national level common framework for Cyber Insurance aligning with the Privacy Act and Mandatory Data Breach Notification with a room to expand to include any future regulatory amendments as well as a regular alignment with the Cyber Security Innovation (new product and service capability).

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

It is important for all organisations at the very minimum to follow the right implementation of fundamental security practices such as password management, configuration management, secure coding, vulnerability management, patch management, and access control. In addition, organisations should focus on cyber security awareness and employee training at all times.

[4] https://www.cyber.gov.au/publications/essential-eight-explained

When it comes to general public who use personal computers and devices connected to Internet, vendors of software and hardware and local communities backed by the state governments should conduct regular booths in the communities focusing on cyber security training and awareness programmes. Phishing in various forms is a common social engineering attack which targets computers and networks by enticing the users to download malicious software or click on malicious links and there is no better way to prevent that by being able to distinguish between legitimate communication and malicious communication over email, phone or any social media. Online cyber security portals can be launched by the State Governments to educate general public on cyber security.

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

Cyber security awareness and training for the general public is a change that Government can implement. Local councils should be supported by both the State and Federal Governments and the public themselves to raise this awareness with some basic cyber security training including curbing natural tendencies and emotional reactions to various forms of social engineering tricks, demonstrating simple mock social engineering attacks, secure use of internet and services, and checking on regular software updates on their personal devices. Similar to joint cyber security centres that engage Government and Industry, security centres at councils that engage general public need to be developed to touch on this awareness at the grass root level. State Governments can launch online portals for general public to improve their cyber security awareness.

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

One approach is to utilise cyber ranges to develop a valid private network attack simulation model with high accuracy and performance. This demands good research collaboration between the owners of private networks, Government and research institutes to be able to develop appropriate solutions that can be standardised industry-wise.

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

Private networks that converge OT systems with business IT systems are considered as most critical systems and require stronger cyber defence. These industries include mining, energy & resources, utility, oil & gas and transportation. A cyber attack on these industries not only degrades the availability and integrity of critical systems but also can severely impact human lives.

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

For Australia to be a safe and secure smart nation, it is highly important for us to focus and strengthen on our research & innovation (R & I) capability, standardisation process, cyber regulatory frameworks, supply chains within local operations and across international borders, and so on.

We would like to respond on the R & I aspect as others were discussed mostly in other parts of this report. From Cyber Security R & I perspective, we are behind several developed and developing economies albeit having strong and growing research community in cyber security and reasonable funding sources from the Government. We believe the following funding models can be explored:

- It is important for Australian industry (including Banking & Finance, Retail, Energy & Resources, Transportation & Hospitality, Utilities, Mining and IT & Security Services) to engage with the Government and Academia on a cyber security roadmap that can uplift their capabilities to be resilient against cyber attacks including unknown ones and need to engage in the Government supported initiatives such as Cyber Security CRC.

- While Government offers Linkage grants to support projects between academia and industry, our understanding is that we need to have a funding model to facilitate the exchange of problem statements and discussions around their value that fit into the roadmap of the industry. Often, background works that shape the proposal for funding, especially when the proposal won't get through, might not be well received and appreciated by the funding sources. We need to pursue for a cultural change in the funding model to eliminate this "initial dilemma". While Cyber Security CRC addresses this to some extent, we need to adopt this model for other types of research grants.

- As remarked in (11), Government should encourage multi-national companies with strong presence in Australia to open Research & Innovation Labs focusing on cyber security and adjacent domains meeting the needs of Australian market and contributing to cyber security industry growth by providing them with relevant tax incentives. It also provides an opportunity for the Government to capitalise on the global innovation capabilities of these companies that can significantly foster Australia's innovation footprint.

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

For industry cyber security is essentially a business problem and looks for adopting solutions that not only addresses cyber threats and vulnerabilities but also provides a competitive edge. Businesses make investments in cyber security technology accordingly. While it's no longer an "after-thought", cyber security adoption and innovation are driven by businesses needs and competitive gains from other similar businesses.

For Government, protecting infrastructure and various business services against cyber threats and vulnerabilities is a national priority. It is important for any nation to demonstrate to the world that it is a trusted, safe and secure place for investors, thus contributing for their prosperity and economy and Australia is no exception to that.

This difference in the perspective of cyber security between industry and Government is a big barrier for information sharing between them.

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

    The extent to which the lack of cyber awareness drives poor consumer choices and market offerings depends on whether the consumer is a B2B or B2C.

    In the case of B2B, rather than cyber awareness, it is the lack of capability or not allowing sufficient time to do a proper security check which can lead to poor procurement of products and services. For example, there are several new products out there in the market that claim Artificial Intelligence (AI)/ Machine Learning (ML) capable cyber security solutions for threat analysis, vulnerability management, and other cyber tasks. Unless sufficient due diligence is done on their capability, there is every chance for a B2B consumer to make a poor choice.

    In the case of B2C consumers (e.g. retailers, consumer product companies), especially during digital transformation of businesses, consumers' lack of cyber awareness drives the selection of poor choices. This includes, for example, purchase of IoT devices without proper security configuration and registering for online business services that do not offer proper authentication mechanisms and privacy assurances.

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

    Increased consumer (especially B2B) focus on Australian cyber security products would provide a great competitive edge for these products in the local and international markets. Moreover, these products can be sold in other countries through several international IT Services and Cyber Security services companies operating in Australia who already have a strong global presence.

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

25. ***Would you like to see cyber security features prioritised in products and services?***

    Yes.

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

    No.