Submission No 15

INQUIRY INTO CYBERSECURITY

Name: Professor Vijay Varadharajan

Date Received: 19 September 2020

Hon Tara Moriarty MLC
Committee Chair
Portfolio Committee No. 1 – Premier and Finance| Upper House Committees |Legislative Council
Parliament of New South Wales, Parliament House, Macquarie Street Sydney NSW, 2000 Australia

Dear Hon Committee Chair,

I would like to thank the NSW Legislative Council's Portfolio Committee No. 1 – Premier and Finance for inviting me to make a submission to the inquiry into Cybersecurity.

I am Professor Vijay Varadharajan, Global Innovation Chair Professor in Cyber Security and the Director of Advanced Cyber Security Engineering Research Centre (ACSRC) at the University of Newcastle. I have had experience in Cyber Security both in industry and academia, internationally and nationally, over the last 35 years. I have been a member of several Cyber Security Advisory Boards at leading technology companies internationally such as Microsoft, SAP and Hewlett-Packard, as well as member of Government Advisory Groups and Committees in the UK, European Union, Australia and India.

As part of this submission, I will be addressing the following aspects of cybersecurity, which I feel could be of relevance to this inquiry.

(a) Cybersecurity Context
(b) Comments on some specific aspects raised by the Terms of Reference
(c) Further suggestions in Cybersecurity for NSW Government

(a) Cybersecurity Context

It is clear that technology has become pervasive in our daily lives and will continue to do so even more in the foreseeable future. In particular, the combination of technologies Internet of Things (IoT), cloud infrastructures, and big data applications and services, together with cyber physical systems will be dominating the technology space for many years to come. We believe this dramatically increases the ***cyber security threat velocity*** – with (i) more and more vulnerabilities and attacks arising with different technologies (e.g. due to systems of systems), (ii) an evolving set of bad guys (e.g. from hacker groups, to corporate espionage, to state actors), (iii) attacks happening at zero time (with no grace period) and (iv) attacks becoming sophisticated due to easy availability of advanced tools. This is the cyber threat environment we find ourselves in. As mentioned above, all the parties involved (government agencies, industry and users) need to play their parts in containing and mitigating the cyber security threat velocity in such a pervasive technological environment

(b) Aspects addressed in the Terms of Reference

In this overall context, the Terms of Reference raises some important issues for New South Wales such as the need for cybersecurity policy framework and effective response and mitigation measures to counteract increased level of cyber incidents and data breaches. In this section, I provide my observations and comments on some such specific issues.

(i) Cyber Incidents and Data Breaches

In Nov 2019, the Auditor General reported that there had been more than 3300 data breaches across NSW agencies as of March 2019[1]. Several NSW agencies also experienced cyber incidents such as Transport for

[1] https://www.smh.com.au/national/nsw/nsw-government-was-warned-over-cyber-security-weaknesses-20200620-p554iu.html

NSW – August 2020[2], Service NSW – May 2020[3], NSW Labour Headquarters – November 2019[4], Revenue NSW – June 2019[5], Department of Planning and Environment – January 2019[6] and Family Planning NSW – May 2018[7].

Such cyber incidents and data breaches have become common all over the world over the recent years. In the future, this trend will continue with the threats becoming more automated, more intelligent, and disruptive and even more destructive. Nation-state actors are likely to push the envelope and use cyberattacks against critical infrastructures to achieve greater strategic effects than through traditional means. Criminal actors will also take greater advantage of the explosion in consumer focussed apps such as in fintech and healthcare sectors. The ubiquitous low-cost Internet of Things devices, current being shipped with almost no security, can have major harmful effects in applications such as smart cities and smart infrastructures (especially using technologies such as 5G). It is likely that there will be greater emphasis on data centric cyberattacks as data becomes the new currency in the digital world. Understanding which data moves where and how in organizations is key, especially as attacks will focus more and more on data itself.

Therefore, it is vital that the NSW Government agencies going through digital transformation processes to take every security precaution that is possible to reduce the probability of such occurrences. In the world of cyber security, there is no such thing as absolute security. Each agency should set cybersecurity as a strategic priority and have a cybersecurity policy framework. This should be a "living" framework continually being updated. In fact, it is important for NSW Government as-a -whole needs to have an overarching cybersecurity framework, which each agency can instantiate, considering their own specific circumstances and environments. What is even more critical is processes and procedures enforcing the deployment of these security measures throughout the NSW government.

At the higher level, these cybersecurity frameworks suggest policy profiles and guidelines, while recommending specific security measures at the lower level. There are several cybersecurity frameworks available both internationally and nationally recommending various specific security measures to help reduce the potential of cyberattacks. The set of security measures from the Australian Signals Directorate referred to as Essential 8 provides a good starting point and can potentially help to mitigate many commonly occurring cyberattacks. Key security measures amongst these is the need to continually patch applications and operating systems, ensuring least privilege (only those who need access to applications and services should be given the privileges), multi-factor authentication as well as application whitelisting and appropriate configuration of applications.

---

[2] **Transport for NSW – August 2020**

- Over 54,000 scanned NSW driver's licences found in open cloud storage – TfNSW investigates mystery data leak on AWS S3
- Service NSW still waiting to notify on data breach after four months
- Data breach exposes tens of thousands of NSW driver's licences online

[3] **Service NSW – May 2020**

- Service NSW hit by email compromise attack | Agency tries to work out what they accessed

[4] **NSW Labor Headquarters – November 2019**

- NSW Labor Headquarters Reported for possible Data Breach

[5] **Revenue NSW – June 2019**

- Privacy fears for Illawarra drivers as NSW govt data breach referred to ICAC Illawarra drivers may have had their private details leaked to the media as part of a "political smear campaign"

[6] **Department of Planning and Environment, NSW Major Projects – January 2019**

- Fury over privacy 'breach'. FURIOUS Tweed Valley Hospital site protesters say their privacy has been breached after a State Government body allegedly published their personal details online without permission.

[7] **Family Planning NSW – May 2018**

- Family Planning NSW hit by ransomware attack – may have compromised online databases.

(ii) Monitoring and Response to Cyber Incidents

Each agency should have a well-defined set of measures and practices, based on the cybersecurity policy framework mentioned above, to detect and respond effectively to threats and data breaches. Furthermore, there must be clear procedures established for trusted sharing of information between the agencies. I would also strongly recommend a whole-of-government overall cybersecurity capability to detect and respond effectively to cybersecurity incidents.

I note from the report by the Auditor-General for New South Wales (March 2018)[8] actions need to be taken to improve the trusted sharing of information on incidents amongst agencies. Furthermore, the report mentions that some agencies have poor detection and response practices and procedures. I am aware that a Government Chief Information Security Officer (GCISO) had been appointed to address these issues and improve cyber security capability across the NSW public sector. I am confident that after this appointment, the status would have much improved. However, the current state of preparedness is not visible to me.

From my perspective, it would be good for the parliamentary committee to have a progress report on the following aspects: (a) what procedures/protocols and systems have been developed to improve the trusted sharing of threats and security incidents impacting multiple agencies, and what response mechanisms have been established and what lessons have been learnt from post-incident reviews, (b) what security technologies and mechanisms have been put in pace to assist agencies (that have been performing below par) to improve their detection and response capabilities, (c) what governance structures have been established at the whole-of-NSW-government level and what reporting and monitoring mechanisms have been established at the strategic level, and in particular (d) what strategies, governance structures and coordination mechanisms have been established to deal with any major cyber security crisis were it to occur affecting NSW Government organizations - protecting the community from potential harmful consequences, ensuring business continuity, coordinating flow of information between agencies etc.

Equally important are the links with Australian Government security agencies (such as ACSC) as well as with other states and the private sector, both in terms of trusted sharing of information as well as learning from each other's cyber experiences.

Security incidents and breaches can cause extensive damage not only to the bottom line but also to the reputation of an organization. From the Board or NSW Government perspective, what is required is measurable improvements that are consistent in response to security over time. Critical factors include employing people with the right skills and upskilling existing workforce, procedures and technologies for limiting the damages when incidents occur, with the overall aim being long term protection as opposed to just reactive responses.

In this regard, in my experience, the establishment of a thought leadership group with selected people from government, academia and industry, solely based on proven expertise and track record in cybersecurity at the peak level could be very beneficial to the NSW Government in terms of looking at future cybersecurity trends over the horizon as well as helping to formulate appropriate strategies and plans[9].

(c) Further Suggestions in Cybersecurity for NSW Government

I would like to conclude by making a couple of suggestions where NSW government can take a leadership role in cybersecurity, in the provision and maintenance of a safe and trusted environment for the community to carry out its activities in the digital ecosystem.

---

[8] https://www.audit.nsw.gov.au/sites/default/files/pdf-downloads/Final%20report%20-%20Detecting%20and%20responding%20to%20cyber%20security%20incidents%20-%20Web%20version.pdf

[9] NSW Govt has previously used effectively such high-level strategic groups, for instance, NSW ICT Panel in 2014-1015.

(i) *Security and Trust on IoT devices*: As mentioned above, the proliferation of devices being connected to the Internet is leading to amplification of threats and attacks in the digital infrastructure. We have deliberately highlighted the IoT technology due to its ubiquitous connectivity (and use of other powerful capabilities such as cloud) is forcing us to reconsider our definitions of sectors, perimeters, trust, and control.

We believe there is an opportunity for the NSW government to take a leadership role in developing, establishing, and maintaining mandatory minimum standards in cybersecurity of IoT products and its applications. Government is often the single largest procurer of products and services in a state/country. In this capacity, NSW government has a significant influence in getting manufacturers to modify standard security practices as well defining the security requirements. A government-defined minimum standard for cybersecurity in IoT products (e.g. demonstrated by a manufacturer prior to government procurement) can have a significant impact on ensuring that these products are available to everyone. The (initial) minimum standard will become the basis for further enhancements in the future. It will serve as a standard against which manufacturers can be made liable for delivering insecure products. A closely related issue is that government funded projects should be examples of excellence thereby government leading by example in cybersecurity. (Note every security breach in government projects amplifies the failure of government in cyber security).

Governments have long had an important role in maximizing social welfare (e.g. in regulating safety) whereas private sector providers do not have adequate incentives to do so. The social welfare goals (whether free-standing or sectoral) will typically be some mix of safety and privacy. For instance, the former is likely to be dominant in the use of devices in transport while the latter may be more important in healthcare (e.g. medical devices). In the utilities and energy sector, such as smart devices, several goals can come into play; for instance, we do not want these devices in our homes to cause fires, or to leak personal data, or even to enable a foreign power to threaten to turn them off, to allow the utility to exploit market power, to make electricity theft easy, or to make it impossible to resolve disputes fairly.

(ii) *SME and Supply Chain security:* As most systems consists of many components/products coming from different manufacturers and providers; furthermore, many of these components/products are being manufactured by SMEs which form a lion share of the Australian economy. In fact, many of the SMEs may be involved in the development of IoT products in (i). Despite their often-constrained resources, SMEs are essential stakeholders in any effort to enhance cybersecurity—particularly in light of their role in the supply chain—and their needs must be better addressed. The focus on the supply chain security can help to mitigate one of the root causes of the proliferation of security threats in the digital ecosystem. *Once again, we believe there is an opportunity for the NSW Government to take leadership in enhancing the cyber capability of SMEs especially in the regional areas.*

SMEs are often time poor, cash flow poor, limited staff expertise and focused on their current products and services. We believe what is needed to enhance their competitiveness in terms of cyber security are: strategic advice and thought leadership on security best practice, targeted and specialized security training, expertise to their current and future solutions via R&D and innovation, improved engagement with government agencies.

We are currently engaged in enhancing the cyber capability of the SMEs in the Hunter and Newcastle region. We are in the process of developing a Hunter Cyber Hub in collaboration with the Advanced Cyber Security Engineering Research Centre at the University of Newcastle. Supporting the growth of such regional cyber hubs by the NSW government can act as an enabler for growth in the NSW regions not only leading to innovative products and solutions in the cyber space but also helping to improve the job market. This has the added benefit of reducing cybersecurity compromises and vulnerabilities thereby improving the safety of the overall digital ecosystem.

Wishing the best to the committee for a successful outcome.

Vijay Varadharajan FIEE, FACS, FIEAust, FBCS, FIMA, FIETE 19 Sept 2020

Global Innovation Chair Professor in Cyber Security, Australia
Director of Advanced Cyber Security Engineering Research Centre (ACSRC)
The University of Newcastle, Australia

Webpage: https://www.newcastle.edu.au/research-and-innovation/centre/advanced-cyber-security-research-centre/people/professor-vijay-varadharajan-biography