Submission No 26

INQUIRY INTO CYBERSECURITY

Organisation: Palo Alto Networks

Date Received: 2 October 2020

2 October 2020

Portfolio Committee No. 1 - Premier and Finance
Legislative Council
New South Wales Parliament
Submitted via email: portfoliocommittee1@parliament.nsw.gov.au

Re: Submission - Portfolio Committee No. 1 - Premier and Finance Inquiry into Cybersecurity

Palo Alto Networks appreciates the opportunity to provide input to the *NSW Legislative Council Portfolio Committee No. 1 - Premier and Finance (the Committee)* inquiry into cybersecurity. We welcome the Committee's interest in this important subject matter.

Palo Alto Networks is the largest cybersecurity company in the world. Palo Alto Networks secures the networks and information of more than 75,000 enterprise and government customers in 150+ countries to protect billions of people globally, including in Australia. 95% of the Fortune 100 and more than 71% of the Global 2000 rely on us to improve their cybersecurity posture. We work with some of the world's largest organisations across all industry verticals, including government. We combine our knowledge from working with customers and governments across the world to directly inform our responses. We have addressed some of the Committee's terms of reference below.

Terms of Reference Items and Key Recommendations

(c) The policies and procedures underpinning the management of digital information by the NSW Government;

Recommendation: Make Cybersecurity a Key Pillar of the Government's Digital Transformation Agenda. We are pleased to see the NSW Government taking advantage of the benefits of the digital era, including with respect to the digitisation of Government services. In the course of the last year, we have seen the NSW Government move more and more data online, from digital drivers' licenses, to an online death notification service, to the provision of online school enrollments.

However, as the NSW Government moves these services and data online, it is critical that they are secured. News outlets have reported that many people were concerned by public reporting of 54000 NSW drivers licenses that were found in the public domain.[1] This data, which includes the personal identifiable information (PII) of thousands of NSW citizens, is very likely of interest to a range of cyber adversaries. In particular, cybercriminals are attracted to drivers licenses as they can be leveraged to steal identities and access bank accounts.[2] It is therefore crucial that the Government's policies and procedures underpinning the management of digital information have cybersecurity as a key pillar. We note that the NSW Government has recently called for views on its forthcoming *2020 Cyber Security Strategy*. However, to affect cultural and practical change, cybersecurity should be referenced in all Government digital transformation policies and procedures.

[1] https://www.itnews.com.au/news/over-54000-scanned-nsw-drivers-licenses-found-in-open-cloud-storage-552544
[2] https://www.abc.net.au/news/2019-09-06/drivers-licence-identity-theft-leaves-victims-exposed/11439668

Recommendation: Accelerate NSW Government's Safe and Secure Move to the Cloud. Like many governments, the NSW Government would like to transition to the cloud. However, for many governments (as well as organisations generally) there is often confusion or a misunderstanding about how to move to the cloud safely and securely. All organisations must understand that cloud security is a shared responsibility between themselves and their cloud vendor. Cloud service providers (CSPs) are responsible for securing their cloud infrastructures, but the organisation (including government) is responsible for the security of its own data stored in the cloud.

In addition, the NSW Government should remain open to using cloud services located both inside and outside Australia's borders, as long as the data is secure. Often a safe or secure move to the cloud is incorrectly viewed as being synonymous with using onshore cloud services. However, moving to the cloud securely depends on how the information is secured, regardless of location.

The NSW Government, in line with national guidance, should raise awareness on the steps its government agencies should take to move to the cloud securely.

Recommendation: Update the *NSW Government Procurement Policy Framework* to Reference both Cybersecurity and ICT Supply Chain Security. It is important to remember that price should not be the only factor when procuring ICT and cybersecurity goods and services. Governments should be required to consider other, non-financial factors, including cybersecurity and supply chain security. Cyberthreats and supply chain risks continue to emerge and are a concern to governments worldwide.

The Federal Government has made it clear that Australian Governments at all levels are regularly targeted by cyber adversaries.[3] The NSW Government and its agencies are not immune to this trend. At the same time, we have seen public reporting of supply chain vulnerabilities. One of the most well-known was the 2017 NotPetya attack, in which a threat actor compromised the infrastructure of a software provider, tampered with the software, and pushed the tampered version of the software to the provider's clients as a legitimate software update.[4] The NotPetya attack was estimated to have cost approx $10 Billion USD, took a nuclear power plant offline, affected several government ministries and impacted a range of businesses from multinational law firms to factories.[5]

Another important component of supply chain security is source code. In particular, there are security implications of using products or services from companies who share the source code of their unique intellectual property (IP) with governments as a condition of access to their market. Disclosure of this nature can weaken security – as it allows these governments to understand the workings and vulnerabilities of the software or product in question (which may be used by customers across the world). In response to this issue, the United States (US) Department of Defence requires vendors to disclose whether:

1) it has provided source code of its "non-commercial," ie custom, products to any country in the last 5 years, or is obligated to do so in the future; or

2) whether it has provided source code of any of its products (not limited to non-commercial) to any "countries of concern" in the last 5 years, or is obligated to do so in the future.[6]

[3] https://www.pm.gov.au/media/statement-malicious-cyber-activity-against-australian-networks

[4] https://www.enisa.europa.eu/publications/info-notes/supply-chain-attacks

[5] https://www.theguardian.com/technology/2017/jun/28/petya-cyber-attack-cadbury-chocolate-factory-in-hobart-hit-by-ransomware; https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[6] For more information see: US National Defense Authorization Act -https://www.congress.gov/bill/116th-congress/house-bill/2500

At a Federal level, Australia has already established international leadership on supply chain security via its initial approach to 5G supply chain issues. We would encourage the Governments of Australia, including in NSW, to continue this leadership and look at adopting similar measures to those in the US to ensure their supply chain security. NSW should also consider prioritising ICT vendors' ability to demonstrate product integrity and secure supply chain practices, including how a company manages end-to-end risk across its supply chain in its procurement policies and RFIs.

Recommendation: Help NSW Government Agencies Shift to Remote Work Securely. Like many Australian organisations, the NSW Government has needed to adjust as its government entities and employees shift to remote working. As a result, offices, data centres, and remote access/home offices must now be secured in different ways. All individuals have critical roles and responsibilities for securing their organisations. We note that the Federal Government has issued guidance to Australian business and individuals with security tips for remote working. We would encourage the NSW Government to leverage this guidance, and also incorporate this cybersecurity advice into its own online guidance on COVID-19 working from home arrangements.[7] NSW could also leverage the work that international agencies,[8] and industry have done in this regard: Palo Alto Networks has issued its own guidance, for example.[9] Such guidance will have long-standing value and should be updated as needed: many people are acknowledging that even after the COVID-19 crisis abates, remote working will stay a way of life, even for governments.

Recommendation: Issue a Public Service Directive that Cybersecurity is Included in all NSW Government Policies. Technology permeates every aspect of our lives, and every aspect of Government and its functions - from healthcare, to transport and even issuing the NSW drivers license referenced above. It is therefore critical that cybersecurity be a key consideration addressed in all NSW Government policies, unless a reasonable exception applies.

(h) Contractual arrangements between the NSW Government and providers of digital services and infrastructure, including:

(i) Provisions relating to cybersecurity generally; and

(ii) Reporting obligations and the monitoring of cybersecurity incidents;

Recommendation: Note the Complexities of Defining a "Cyber Security Incident". When it comes to reporting cybersecurity incidents it is important to get the thresholds right. If the NSW Government intends to introduce new reporting obligations there can be lessons learned from other policies and regulations. For example, under Australian Prudential Regulation Authority (APRA) regulation CPS 234, companies are required to notify APRA of actual or *potential* compromises of information security. "Potential" is not well defined, resulting in confusion in the financial and cybersecurity industry. For example, is the release of a software vulnerability or a patch (a frequent occurrence) classed as a "potential" compromise? What about a widespread phishing campaign that was blocked before affecting an organisation? Palo Alto Networks recommends that any reporting obligations on

[7] https://www.nsw.gov.au/covid-19/safe-workplaces/employers/working-from-home
[8] https://www.cisa.gov/telework and https://www.nist.gov/blogs/cybersecurity-insights/telework-security-basics
[9] https://blog.paloaltonetworks.com/author/ryan-olson/

cybersecurity incidents should be carefully defined and considered. We also recommend engaging with other jurisdictions (such as the Federal Government) and cybersecurity companies,[10] so as to avoid replicating issues that have arisen in other contexts.

(i) The extent and impact of outsourcing of government information systems, including:

(i) Outsourcing to entities which are owned overseas;

(ii) The risks involved with outsourcing government information systems.

Recommendation: Focus on Vendor and Product Integrity When Outsourcing Systems. There are a range of reasons why the Government may look to outsource its government information systems to entities which are owned overseas. The jurisdiction of the ownership of an entity does not necessarily dictate the security outcomes. When it comes to ICT, we note that some of the companies at the cutting edge of technology and security innovation are foreign-owned companies. We believe that relying exclusively on home-grown technologies will not be as effective as identifying vendors and technologies built upon the highest standards of product integrity and supply chain best practices.

There are important ways governments can establish confidence in vendors regardless of where they are located. We would encourage the NSW Government to focus on vendors' ability to demonstrate strong product integrity and supply chain practices including looking at not only how and where their products are developed and manufactured but also how a company manages end-to-end risk across its supply chain. We would recommend the NSW Government focus on implementing these measures as part of its procurement processes (see above response to “c”). This is a very effective way to increase the level of trust in the security of the technology procured and employed to defend the Government’s information networks and critical mission systems.

Recommendation: Maintain a Free and Open Market. Palo Alto Networks supports Australian cyber innovation and believes that we need more, not less, companies innovating and inventing new ways of combating cyberthreats. However, we caution against protectionist policies that discriminate against non-Australian companies. We believe that healthy market competition drives innovation and we attribute much of our company’s success to the fact that we have had to constantly grow and out-innovate our competitors and meet the market's needs.

(j) The support provided by the NSW Government to local councils and other organisations in

relation to cybersecurity;

Recommendation: Provide Cybersecurity Education and Consider Funding for Small to Medium Enterprises (SMEs) and Local Governments to Improve their Cybersecurity Posture. In order to uplift the cybersecurity posture of SMEs and Local Governments at scale, the NSW Government should work with Managed Security

[10] Cybersecurity companies are regularly asked how they will support customers’ compliance with these kinds of regulations/reporting requirements.

Service Providers, CSPs, ISPs and cybersecurity companies to identify and/or create tailored offerings for SMEs and Local Governments that are cost effective and provide holistic security, alleviating some of the technical burden currently facing Australian SMEs. The Government could look to subsidise the cost of purchasing these offerings via a cybersecurity grants program.

The Government should also work with the private sector to educate SMEs and Local Governments on cybersecurity. Many private sector cybersecurity companies would be able to assist in this regard – for example, Palo Alto Networks offers a range of cybersecurity education and training initiatives. This type of educational/training expertise could be leveraged to support the Government's efforts to reskill/upskill SMEs and local Governments.

Recommendation: Help NSW Enterprises, Schools, and Individuals Understand How to Shift to Remote Work and School Securely. In line with our recommendation at item (c), we would encourage the NSW Government to provide guidance to the broader community - including private industry, schools and individuals - on security tips for remote working or schooling. As many continue to adjust to their new ways of working or learning, it is important that they do so securely. State level guidance and advice can help NSW industry achieve this.

Recommendation: Review "Essential" Sectors (or Functions) in NSW and Reprioritise Cybersecurity Efforts Accordingly, in Collaboration with the Federal Government. The NSW Government has designated certain sectors of its economy as "critical infrastructure," a designation that brings with it prioritised government focus for protection and assistance, including in terms of cybersecurity resources (such as cyberthreat sharing, and other operational assistance). The COVID-19 crisis has reshaped many governments' thinking on what sectors are considered "essential." In many parts of the world, governments have applied this designation (at least temporarily) to grocery stores / the food supply chain, retail, and manufacturing; in some cases definitions have evolved from being primarily 'sector'-based to 'function'-based, in the belief that this approach more accurately conveys the interconnectedness of modern supply chains. In line with the Federal Government, the NSW Government should take a fresh look at the sectors (or functions) that might now be considered "essential" under existing policies and legislation, including the *NSW Critical Infrastructure Resilience Strategy* and reprioritise its cybersecurity efforts accordingly.[11]

(k) The NSW Government's response to cybercrime in the community generally;

Recommendation: Invest in Law Enforcement and the Justice System. Unfortunately, cyberthreats are a ubiquitous and ever-expanding part of modern life. In 2018, close to one in three Australians were victims of cyber-crime.[12] The Australian Cyber Security Centre (ACSC) receives a report of cyber-crime every ten minutes.[13] These attacks come at a significant cost to the Australian economy and our society. They also breed a lack of confidence and faith in online applications and can slow the adoption of digital transformation. It is estimated that cybercrime costs the Australian economy up to $29 billion per annum or 1.9% of Australia's gross domestic product.[14] Investigating and prosecuting these crimes can be challenging; the Internet has made it easier for

[11] https://www.emergency.nsw.gov.au/Pages/emergency-management/local-government/nsw-critical-infrastructure-resilience-strategy/introduction-local-government-user-resource/critical-infrastructure-resilience-strategy.aspx

[12] https://www.staysmartonline.gov.au/news/reverse-threat-cybercrime/stay-smart-online-week-2019

[13] https://www.zdnet.com/article/australians-are-reporting-cybercrime-activities-once-every-10-minutes/

criminals to commit crimes online with relative impunity - enabling them to mask both their identity and location. Today, transnational criminal networks are in many different countries and even lone hackers route their attacks and activities through different countries. This poses significant challenges for national law enforcement and criminal justice systems.

The NSW Government must invest in its justice system accordingly. In particular, we would recommend the Government consider measures to increase the capacity of law enforcement officials to be able to respond to reports of cybercrime within their jurisdiction. This may mean hiring additional resources, reskill existing law enforcement officials on cybercrime or looking to update the ICT systems and applications that support NSW law enforcement investigations. Given the unique challenges of prosecuting cybercrime, we would also recommend cyber education programs for prosecutors and the courts.

Recommendation: Continue to Promote Greater Public-Private Sector Voluntary Sharing of Cyberthreat Information. Voluntary cyberthreat information sharing is critical in understanding the threats, protecting information and networks, and preventing successful cyberattacks. As a result of their worldwide operations and customer base, global cybersecurity companies can have visibility of cyberthreats that rivals some nation states. And in some cases, companies can prevent cybercrime before the victim is aware anything has occurred. Cybersecurity companies often share the forensic information with law enforcement so they can arrest and prosecute the actors behind the campaigns. Strong public and private cooperation are crucial to address the growing threat cybercrime poses to Australia.

The NSW Government should educate Australian organisations as to the value of voluntarily sharing cyberthreat information to prevent attacks; promote the expansion of information sharing organisations across all industry sectors; and encourage all participants to increase the maturity level and effectiveness of threat sharing, and make it more operational and actionable, via automation and real-time feedback loops.

Recommendation: Partner with Industry on State-Wide Cybersecurity Education and Awareness Campaign. The NSW Government has an important role to play in educating and making its citizens aware of the cyberthreats and what steps they can take to mitigate these. The NSW Government could consider launching a large-scale, state awareness campaign in collaboration with the private sector.

(l) Any other related matter.

Recommendation: Strengthen Public-Private Partnerships on Cybersecurity. Regular interaction and consultation between industry and government brings a myriad benefit on both an operational and policy level. The NSW Government should establish new structures to allow the NSW public and private sectors to interact in an ongoing, consistent, and practical way to share ideas and new developments. Suggestions include creating an industry advisory board to support and deliver the NSW Strategy. To maximise industry engagement, we would suggest thematic sub-working groups or that panel membership be on a rotational basis. The NSW Government may also wish to consider how it could leverage NSW Government and industry co-location centres, including the Federal Government's Joint Cyber Security Centre. Finally, the NSW Government could look to establish cyber industry placements in key NSW Government cyber agencies to encourage cyber policy and operational cooperation.

[14] 2020 Cyber Security Strategy, https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy

Recommendation: Strengthen Cyber and Technology Courses in NSW Schools. Addressing cyber education in primary school, all the way through to the university and TAFE sector will be critical to the success of Australia's next generation. This may involve strengthening the NSW schools curriculum to increase focus on cybersecurity courses; in particular, a focus on automation, machine learning and artificial intelligence (ML/AI) is critical, as we know that cyberattacks are increasingly automated and consequently, so must our cyber defences.

Recommendation: Leverage Our Existing Cyber Workforce and Students via an NSW Civilian Cyber Corps. The NSW Government should consider how to leverage its existing cyber workforce and cyber students in support of improving the State's resilience, via establishing a "civilian cyber corps". Civilian cyber corps are civilian organisations that professionally engage volunteers in public interest cybersecurity work and are akin to a Cyber State Emergency Services. These corps can be leveraged to lift NSW's cyber resilience in three key areas: Community Education and Outreach; Testing, Assessments and Exercises for Organisations; Provision of Expertise and Emergency Response. Both University and TAFE students could be leveraged in support of the civilian cyber corps. A civilian cyber corps could help NSW improve its cyber resilience.

Recommendation: Explore Public-Private Partnerships to Reskill and Educate NSW. Many private sector cybersecurity companies offer free equipment, training courses, and/or curriculum to academic institutions, which could be leveraged to support the Government's efforts to reskill NSW. For example, the Palo Alto Networks Cybersecurity Academy Programme provides accredited academic institutions (including secondary schools, TAFEs and Universities) with faculty training, hands-on labs, modularised curriculum and virtual firewalls at no cost. We have 24 academy partners in Australia and one in NSW; we would be pleased to add more academic institutions to our programme. Government and private industry could also explore co-funding education initiatives, including scholarships or training programs.

Conclusion

As the Committee embarks on its inquiry into cybersecurity, Palo Alto Networks is ready to contribute our expertise and experience. We would be happy to discuss our ideas further. For more information, please contact Sarah Sloan, head of government affairs and public policy, Australia and New Zealand, at and Sean Duca, chief security officer, Asia Pacific & Japan, at .

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the future with technology that is transforming the way people and organisations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seises the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of security, protecting tens of thousands of organisations across clouds, networks, and mobile devices.

Palo Alto Networks is committed to helping the Australian Government and private organisations across all industry sectors embrace the digital world safely and protect their business operations from cyberattacks. Many of our customers are Australia's largest enterprises and government organisations. We also have undertaken a range of activities that contribute to strengthening Australia's cybersecurity posture, including hosting roundtables with government and enterprise stakeholders to promote thought leadership; and partnering with the education sector to design cybersecurity courses. For more information see https://www.paloaltonetworks.com.au/