Office of the Victorian Information Commissioner

t 1300 00 6842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D19/5886

15 November 2019

Cyber Security Policy Division
Department of Home Affairs
4 National Circuit, Barton, ACT 2600

Australia's 2020 Cyber Security Strategy – *A call for views*

Thank you for the invitation to make a submission to your review of Australia's Cyber Security Strategy.

My office, the Office of the Victorian Information Commissioner (**OVIC**), has a unique regulatory focus, with combined oversight over privacy, information security and freedom of information in Victoria, administering both the *Privacy and Data Protection Act 2014* (**PDP Act**) and the *Freedom of Information Act 1982* (Vic).

Under the PDP Act, my office is responsible for monitoring and assuring the security and integrity of public sector data, including law enforcement data systems and crime statistics data, as well as auditing such use under the Victorian Protective Data Security Framework (**VPDSF**)[1]. The VPDSF, implemented under Part 4 of the PDP Act[2], is the overall scheme for managing protective data security risks in Victoria's public sector. As the only jurisdiction in Australia with legislated security standards, OVIC is at the forefront of information security regulation in Australia. It is for this reason that Australia's 2020 Cyber Security Strategy is of particular interest to my office.

This submission will address a number of questions outlined in the discussion paper 'Australia's 2020 Cyber Security Strategy – A call for views' and make recommendations on what the new strategy should consider.

Response to question 1 – What is your view of the cyber threat environment? What threats should Government be focusing on?

In Victoria, the cyber threat environment has evolved dramatically over the past few decades. According to the Victorian Government Cyber Security Strategy 2016-2020, a threat landscape that was once relatively unsophisticated lone actor cyber-hackers is now well-funded by political hacktivists and foreign governments seeking to infiltrate government, businesses, and private networks. In comparison to previous years we are becoming more aware of Government networks in Australia being regularly targeted by increasingly sophisticated cyber adversaries[3]. Furthermore, as public sector agencies seek to digitize more of their service delivery and decentralize data systems, the threat surface area is growing and will continue to do so.

---

[1] For more information on the Victorian Protective Data Security Framework, please see our website: https://ovic.vic.gov.au/data-protection/what-is-data-protection/framework-vpdsf/
[2] PDP Act 2014, s85(1)
[3] State of Victoria (Department of Premier and Cabinet) (2017) "Victorian Government Information Technology Strategy 2016-2020: 2017-18 Action Plan", Victorian Government, retrieved from: https://www.vic.gov.au/victorian-government-cyber-security-strategy

It should be said that while digital technology has its risks, it undoubtedly has its benefits. The rollout of new digital initiatives has, generally speaking, made service delivery more accessible, efficient and cost effective. It's clear that technology has the potential for immense good and will continue to develop and shape the way we interact with the world. The challenge that many organisations now seem to face is how to bring out all this good while minimising the risk to their systems and stakeholders.

Response to question 5 – How can Government maintain trust from the Australian community when using its cyber security capabilities?

Government organisations have an obligation to assure the Australian community that their information is being adequately protected. While this could take a number of different forms, fundamentally governments must have a plan for how they manage their security risks, ensure there will be adequate controls around the lifecycle of information, and that agencies will be able to demonstrate that this work is being monitored.

Internationally, we're seeing significant development in this space. In 2018 Singapore passed its Cybersecurity Act, introducing an information security framework for public sector agencies, licencing requirements and an independent body to investigate cybersecurity threats and incidents[4]. This year, US states have introduced a range of legislation including mandated cybersecurity programs for both public and private entities, blockchain research and development taskforces to better secure government networks, and cybersecurity education suites for schools[5]. Not to mention the GDPR which has had an enormous impact on the protection of personal information and information rights of EU citizens. These developments all seem to point to a growing standardisation around data protection and cyber security. This is taking the form of increased legislation, certification and publication of guidelines.

Standardisation is a positive step towards building trust in a product or service because it establishes a baseline understanding of how things should be. In addition to this, there needs to be an assurance program to demonstrate a level of adherence to the agreed baseline requirements. A system like this would ideally ensure a level of consistency and denote who is responsible for protecting public information.

Victoria's legislated security framework and standards, issued under the PDP Act 2014, leads the way in Australia and goes some way in providing assurance to the public that their data is being appropriately managed by Victorian public sector agencies. Under the PDP Act, Standards are issued which public entities must address in their security programs, the public sector body Head is made to be accountable for data protection within their organisation, and there are annual review periods conducted by OVIC.

It would be worthwhile for the wider government to commit to introducing legislated accountability around the protection of information so that organisations are compelled to handle information appropriately and to develop secure systems. This would promote greater trust in Government and its cyber security capabilities.

Response to question 8 – How can Government and industry sensibly increasing the security, quality and effectiveness of cyber security and digital offerings?

An awareness and appreciation of security needs to be embraced across all security areas, not just **ICT**. This is a point that was somewhat overlooked in Australia's cybersecurity strategy 2016 - 2020. All security areas are equally important for organisations to consider. If a cybercriminal gains unauthorised access to a server room and infiltrates a network, it's just as much a **physical** security issue as a cyber issue. If an employee gains authorised access to a network and uses it for malicious purposes, this may be a **personnel** security issue. If sensitive information is being leaked or miscommunicated, adequate control over **information** security may be lacking. Above all, adequate **governance** arrangements need to be in place to denote who

[4] Cybersecurity Act 2018 (Singapore). Also see https://www.csa.gov.sg/legislation/cybersecurity-act for more information
[5] For an overview of changes in cybersecurity legislation broken down by US state and status, see http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx

is responsible; to document risks, review cycles, policies and procedures; and, ensure adequate information lifecycle and access control and robust HR policies.

Even with the focus on 'cyber' (i.e. electronic information and systems), there are elements of people and process that must not be forgotten. With any approach or initiative that the strategy identifies, the areas of people, process and technology must be considered equally. Even if the system purchased is "secure", the way in which it is used from the end user perspective also plays a role. For example, a device can have the best threat protection mechanisms, but if people are not locking the device after use, it can represent a new set of issues. According to the OAIC[6], 34% for all reported breaches were due to human error and 62% of breaches were due to malicious or criminal attacks, of which almost half were phishing related. These statistics point to an overall lack of cyber hygiene which OVIC also suggests should be considered a focus of the new strategy.

The information security risks that government and businesses face vary dramatically in severity and threat type depending on the nature of the information and the operating environment. There are many considerations that are unknown (or unknowable) until they become an issue, or incident. There is no single technical solution that will solve everything, so the focus should be on addressing security as a risk-based activity and develop strategies that enable organisations to developmentally evaluate and respond to their unique security environments.

While technology firms are good at promoting the technological features their products, it can be challenging for security practitioners to communicate the importance of the security aspects of these products. Outreach initiatives, such as the Joint Cyber Security Centre (a product of the 2016-2020 strategy), have been a positive first step in promoting greater cyber awareness and collaboration for both government and industry. More can certainly be done to engage areas of the community, particular regional and small businesses to improve cyber hygiene and resilience strategies. Future campaigns might include security disclaimers on the use or implementation of good or services; issuance of webcam covers for every laptop purchased; cyber security education programs in schools; incentives for commuters to get mobile phone privacy screens; and, media advertising and awareness campaigns. The focus of these messages should be end user centric and highlight the risks that subscription of digital goods and services have on the integrity of systems and individuals' privacy.

Response to question 10 – Is the regulatory environment for cyber security appropriate?

OVIC's experience is that it is important to build a strong collaborative regulatory environment. Security in practice is risk-based and if the federal government were to implement a regulatory cyber security framework, it cannot be a 'tick and flick' compliance exercise. It needs to be measured and on-going, with respect to the context and value of the information being protected. Different security practitioners work with varying resources, different operating environments and competing priorities where decisions are made based on the level of risk to the business. A prescriptive one-size-fits-all compliance regime will therefore not adequately address security risks in the unique operating environments of individual organisations.

Certification is great for providing a level of assurance in goods, services and systems to government and the end user, however from a regulatory perspective, they can also be a slippery slope a 'tick and flick' mode of compliance. There is a misconception that systems that are 'certified' just need to be installed with nothing further to be considered. We should be wary about falling into this trap. The threat environment is continually evolving, and all organisations should have security programs that are adaptive, suitably resilient, and built with continual improvement in mind. This is why a risk-management approach is crucial. Certification programs are important, but they have a place. Where certification programs exist

[6] OAIC (Aug, 2018) "Notifiable Data Breaches Quarterly Statistics Report: 1 April to 30 June 2019"

there must also be an educational piece about the role of these programs in relation to organisations' information security management frameworks.

Third-Party assurance is an essential component of information security, and an important consideration in how cyber security is regulated. However, it can be difficult to implement in a risk-based model. How does one get consistent assurance that both parties are on the same page? There can be a lot of confusion and disagreement around third party agreements because of different understandings around operating environments, information type, risk appetite and cross-jurisdictional considerations. It is important to highlight that Third-Party Agreements and MOUs are not in themselves the only assurance measure that needs to be considered. Where Agreements and MOUs exist, there also needs to be active monitoring and review to ensure that the original intent of the contracts are met, and that the contract or agreement is still relevant to the organisation's current operating environment.

The regulatory environment in state of Victoria

In Victoria, in-scope public sector agencies are required to comply with **Part 4** of the *PDP Act 2014* relating to Protective Data Security. The VPDSF was established under this part seeking to assist public sector organisations to mitigate security risks across the five security areas mentioned above. The PDP Act also introduces the Victorian Protective Data Security Standards (**VPDSS**) which provides a minimum set of protective data security requirements to follow. The PDP Act designates the public sector body Head as the accountable person for protective data security within their organisation. Additionally, it lists a number of assurance measures that the organisation must undertake, as follows[7]:

- undertake a security risk profile assessment (including an assessment of contracted service providers)
- develop a protective data security plan and address the compliance status (to the VPDSS) of any contracted service provider of the agency
- review protective data security plans every 2 years, or sooner in the event of significant change to the operating environment of the organisation
- submit a copy of the protective data security plan to OVIC

The VPDSF is the first of its kind in Australia. It puts security on the agenda and makes public sector agencies accountable for the way in which they collect, store, manage, use, disclose or transfer data. It also allows a level of oversight for OVIC to perform its regulatory functions while pragmatically addressing state-wide information security risks. Overall, the regulatory environment for information security in Victoria sets a positive precedent for what regulatory reform might look like at the national level.

Response to question 12 – What needs to be done so that cyber security is 'built-in' to digital goods and services?

A policy of security-by-design must be adopted to build good security mechanisms into goods and services. Digital goods and services should not be built in a way that leaves them vulnerable to compromise. Any vulnerability that is intentionally built into a device, whether to be accessible by authorities or the service provider is an exploit that can be accessed and manipulated for malicious intent. It's important that we do everything that we can to build comprehensive and resilient security into digital goods and services. Further, good Cyber Security is not just cyber. A holistic approach is needed involving all domains of security such as physical security, personnel security, information security, ICT security, all underpinned by good governance. All domains should be considered in building security-by-design into digital goods and services.

[7] PDP Act 2014 (Vic), s.89

I thank you again for the opportunity to make a submission on Australia's 2020 Cyber Security Strategy. I look forward to reading the published strategy. If you have any questions about the above or our submission to the DHA, please don't hesitate to get in touch with my colleague, James Dougan – Policy Officer, at [redacted]

Yours sincerely

[redacted]

Rachel Dixon
Privacy and Data Protection Deputy Commissioner