Our Reference: Ref

7 November 2019

Marc Ablong
Deputy Secretary
Department of Home Affairs
National Circuit
Canberra 2600

Dear Marc,

Sapien Cyber Submission – Australian Cyber Security Strategy 2020

Please find attached Sapien Cyber's submission to the Australian Government's Cyber Security Strategy 2020.

Sapien Cyber (formerly Sc8) is founded upon Edith Cowan University's (ECU) 20 years of world-leading research in cyber security, and is ECU's commercialisation vehicle for that research.

Sapien is a commercial entity, bringing together a team of industry experienced practitioners to develop a unique, sophisticated world-leading solution for Operational Technology (OT), Information Technology (IT) and Building Management Systems (BMS) environments.

Our technology platform provides unparalleled visibility, threat detection and response capabilities, reducing our clients' risks through a sophisticated layered approach to cyber security.

We welcome the opportunity to participate and contribute to Australia's 2020 Cyber Security Strategy, with its intent to help build a strong and effective Australian sovereign cybersecurity ecosystem and industry. Such a domestic sovereign Australian industry is essential for Australia's national interest.

While the Commonwealth itself, through ASD and other Commonwealth Agencies and Departments, can both protect key Commonwealth assets and assist where private infrastructure is under acute attack, the support and cooperation of an effective Australian industry is essential to adequately protect the array of important infrastructure assets held in private hands.

This particularly applies to vital or critical infrastructure. With the threats to such infrastructure from both state and non state actors only on the increase, this is not something which either the Commonwealth or Australian industry can do by itself. Cooperation between the Commonwealth and Australian industry on cyber security protection of critical infrastructure is essential in our national security interest.

Sapien's technology platform and suite of managed services were developed in response to the exponential increase in the number of vulnerable internet connected OT devices used in maintaining the ongoing operations of our country's critical infrastructure.

The comparative lack of attention in Australia to OT cyber security by infrastructure providers represents an unacceptable exposure that the 2020 Strategy must address as a priority. We believe that the growth of a sovereign domestic cyber security capability and the protection of Australia's critical infrastructure are foundational to Australia's national interest now and in the future, and that they should be supported and facilitated by the 2020 Cyber Security Strategy.

A detailed response to the 26 questions posed in the Home Affairs Discussion Paper are attached.

We are happy to contribute further in any way that you consider helpful to your deliberations.

Yours sincerely,

[redacted]

Glenn Murray
CEO
SAPIEN CYBER

Attached : Sapien Cyber Submission - Australia's Cyber Security Strategy 2020

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

With technologies continually evolving, combined with a drive towards data-driven and remote operations, there is an increasing convergence of IT and OT systems. This convergence has taken a relatively isolated environment (OT) and connected it via Internet and cloud environments. Consequently, previously comparatively isolated systems are now vulnerable and being actively targeted by cyber criminals. The very real outcome of an attack on these systems responsible for our critical infrastructure are huge impacts on social life, business environments and, ultimately, the economy.

The threats are increasing in both sophistication and frequency, identifying the need to consistently evolve penalties that keep pace with changing cybercrime and deter malicious actors. At the same time, consequences of attacks are increasing in severity, as information systems become more central to business and society. The threats that Government should focus on are those that affect both Information Technology (IT) and Operational Technology (OT) within critical infrastructure, as those are the systems that are essential for supporting the wellbeing and prosperity of Australians.

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

The explanation of responsibilities on page 8 of the discussion paper is largely accurate, although in such a brief description some of the generalisations do not hold true. One key example is in the area of Operational Technology. Operational Technology (OT) refers to the hardware and software used with the automation controls systems within infrastructure. These systems, including Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) are used in multiple industries including critical infrastructure, such as power, oil & gas, water treatment, transportation, defence, traffic control and within building management systems. These industries form part of our national critical infrastructure, without which Australia's society and economy would fail.

The majority of Operational Technology businesses' systems are decades old and aren't monitored nor have they received patch updates since installation.

Protecting those critical systems should be a priority for Government, as society and the economy depend upon them. Additionally, arguably Government responsibility in enforcing the law has to date been constrained to those attacks that have significant impact. Given that the majority of cyber threats originate from international sources it is imperative that Australia continues to work with other nations, e.g. through instruments such as the Convention on Cybercrime, to encourage them to take action where Australia has no jurisdiction, but where Australian infrastructure is impacted by malicious activity.

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

Responsibility should be aligned with the source of the risk. It is not reasonable for the end users to bear responsibility for a security gap that arises from the technology provider. By the same token, it is not reasonable for technology providers to be responsible for inappropriate actions or inactions by the user.

However, technology and security as a service are increasingly provided as 'black box' solutions beyond the capability of the average user. Cybersecurity capability lies within industry and academia, not in the general population.

Therefore, Government should consider working with industry and academia to strengthen the cybersecurity ecosystem and introduce appropriate levels of service and standards to increase public trust in cyber security products and services.

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

Government should have a stronger role in deterring and responding to significant threats to national critical infrastructure. Government needs to give clear identification of the minimum cyber security standards and/or legislation that critical infrastructure operators must comply with. Additionally, Government needs to be clear as to which aspects of national infrastructure are most important to our society and economy, and what it will do if those systems are affected. Finally, there needs to be clear parameters under which fines/penalties, of sufficient level, are enforced to act as an incentive to comply. This would increase public confidence and understanding of the role that Government will play to deter and respond to serious threats.

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

If Government requires access to business systems to increase our national cyber security, then it must maintain trust by holding private and commercial information as sacrosanct. This includes providing clearer definitions around the expectations under the Assistance and Access Act 2018.

Setting public standards and expected levels of service, whilst also maintaining an environment that supports technology development, will create more trust and confidence with the public. Government should clearly detail who can expect what level of service, if they need to call upon Government cyber security capabilities. Public reporting on these services each year would assist to show that Government intends to be held publicly accountable for the cyber security capabilities it provides. As it is unlikely that Government will always be able to deliver sufficient levels of cyber security capability, especially during times of serious threat to the nation's critical infrastructure, Government should consider also what Industry can do to support these efforts and how Industry will demonstrate to Government that it has the capabilities to assist.

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

Absolute protection may not be viable, as noted on page 11 of the discussion paper. However, in situations where protections are limited, the provider should explain to the customer in clear language (and not hidden in large volumes of terms of conditions) where the vulnerabilities exist, what mitigations can be put into place and identify the residual risk. This should include an understanding of the limitations of liability and be accepted by the customer. Setting appropriate legal standards for products and services will help to clarify what is expected of cyber security products and services.

A large volume of cyber-attacks could be prevented by simply putting in place basic cyber security practices. This includes proper use of passwords and ensuring the product is up to date with patches, however despite efforts by ASD to engage businesses, the general public is still not sufficiently aware of the vulnerabilities that exist by not following these basic actions. Hence there needs to be education practices put into place, including introduction into the school curriculum. This would be further enhanced with Government working with industry to build capability and awareness programs.

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

Government and industry have a role to ensure that products and services have a reasonable level of cyber security protection, and that consumers know their rights and risks. Ideally there should be some level of standardisation of these protections and a responsibility from service and product providers to provide ongoing support and awareness as threats evolve. There is a case also for education of consumers on residual risks and how they should mitigate them.

As companies operate across shared digital applications, it is essential to create an ecosystem that promotes an open and trusting relationship between Government, industry and academia focused on cybersecurity.

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

Government and industry might consider a rating system for cyber security protection attributes of offered products and services, so that consumers can make an informed choice.

Increasing cyber security starts by promoting a proactive approach to cybersecurity rather than a reactive approach. For example,

- ensuring that organisations digital offerings secure by design: in the building of technology functionality usually comes first and the implementation of cyber security is either non-existent or is added after the design.
- putting in place effective monitoring solutions within organisation IT and OT networks: within organisations, usually the first indications that a cyber-attack has occurred is due to the effect on business rather than detection of a cyber event.
- digital offering cybersecurity standards be put into place, so that out of the box settings meet the minimum requirements of digital offerings sold in Australia. This includes clearly identifying recommended settings in user manuals in regards to cyber security and privacy settings.

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

Instead of completely devolving functions to the private sector, perhaps consider how Government and Industry can create a cyber security ecosystem to work more closely together to ensure that Government has appropriate visibility of standards of service, and has a mechanism to identify unique cyber security threats and techniques that Industry may become aware of from time to time.

An example relates to the risks in critical infrastructure services. Failure of providers to establish adequate cyber security may justify Government establishing step-in powers. However, through the proposed initiatives in this questionnaire, the need for Government to step-in could be mitigated through sovereign industry participation, providing an informed appreciation of the level of risk and clear advice to providers on required levels of cybersecurity in critical infrastructure.

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

The importance of continuity of the most critical infrastructure sectors, many of which are underpinned by operational technologies (as explained in our response to question 2) , should be appropriately recognised. Addressing the importance of continuity through regulation may help clarify and achieve expected levels of protection for critical infrastructure owner operators. To do this properly would require clear detail of what is required for appropriate levels of protection by sector, reviewing what is currently defined as critical infrastructure. This also would include what Government will do if called upon to assist and should include the role of the cyber security industry in assisting.

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

Government should consider whether cyber security protections such as the ASD Essential 8 mitigations should be the basis for regulated minimum standards for critical infrastructure providers.

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

Government might consider a ratings system that characterises the level of security in a given product or service, determined by assessment that is funded by the product/service vendor. This might be complemented by a regime of penalties for failing to meet a standard, particularly for use of insecure goods and services in critical infrastructure.

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

Government might: establish a trusted supplier list; give priority to sovereign industry; do not allow public sector agencies to procure through grey market channels; utilise blockchain or similar approach to ensure integrity of supply; and, knowing that there will remain untrusted components, develop trusted cyber security systems that can monitor those components.

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

- Ensure that cyber security education starts in early education (primary school level), to create an understanding that good cyber security practice is simply part of using technology. This will also assist to develop early interest in pursuing cyber security as a profession as the student develops;
- Encourage tertiary education in cyber security and consider waiving the higher education cap for associated courses;
- Ensure that tertiary cyber security course curriculums are appropriately accredited;
- Ensure key cybersecurity related positions require appropriate qualifications;
- Encourage Australian cybersecurity companies and help develop an export industry for cyber security;
- Encourage universities to incorporate cybersecurity content into degree unit structures;
- Focus on both TAFE and University qualifications alongside industry accreditation requirements that professions such as accountants or lawyers must comply with to maintain competency; and
- Focus on pathways and opportunities for reskilling of current full-time employees.

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

Australian businesses need to be better aware of their risks, not only based upon existing rates of cyber incidents but taking into account potential future attacks. Clarity may be needed in insurance contracts about at fault liabilities in the case of claims that can be attributed to user actions.

Compliance to cyber security standards and evidence of actively monitoring networks should attract lower premiums. Insurers are aware of the financial risk they are exposed to from insuring non-compliant companies.

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

- More consumer education. Consistent messaging provided using different modalities to ensure the messages are understood and required changes are adopted.
- Government action to systematically attribute sources, and improved relationships with foreign governments to take action against associated actors.
- Improved automated identification of spam/phishing emails across providers by blocking at the network (similar to the UK use case, noting that this only applied to Government sites, whereas the problem is far greater).
-

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

The DFAT International cyber security strategy needs to translate into actionable agreements between nations' law enforcement agencies to prosecute malicious actors. Government might consider what options might be pursued in respect of foreign jurisdictions that routinely fail to address malicious cyber activity that has an impact on Australia.

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

This is where the cyber security Industry can help to increase Government's understanding about threats, as well as to assist essential private networks to be better prepared to defeat malicious cyber activity and recover when an incident occurs. There should be a mechanism in place for Government to create a sovereign ecosystem by identifying those most trusted industry entities that can provide this service. This service should be undertaken as a mitigation to reduce the need for government to exercise step in powers. It will also assist essential private network operators to identify which Industry organisations they should have most trust in. For this type of mechanism to work it would also be essential for Government to clearly identify "essential private networks".

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

These are defined through the Trusted Information Sharing Network. There is a clear case for power and utility service providers, as well as the food chain and the financial systems that underpin the ability of the public to purchase goods and services, to be considered critical systems. Many of these critical sectors are underpinned by operational technologies that are historically less secure as they have been increasingly connected to public networks.

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

The most likely funding model is for additional protections to be paid by service providers and recovered as necessary from customers. However, in the case of power and utility providers who need to improve their security, this would result in highly unpopular increases in utility charges. Instead, these improvements might be supported through Government incentives, which would be a good way of building a sovereign cybersecurity industry capability.

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

Whereas otherwise there would be concerns from industry about sharing such information, we assume that such sensitivities are already being managed within the Trusted Information Sharing Network arrangement and the Joint Cyber Threat Centres. There needs to be a secure forum/platform where approved Industry and academia participants can share data, emerging threats and trends in cybersecurity.

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

We very much agree. This lack of awareness is a combination of poor advice from industry providers and poor awareness of users. Hopefully both of these should improve in future, the latter through better education of younger generations. For example, there is now a cyber element in WA education throughout schooling. A lack of Government standards for cyber security services and products contributes to a lack of understanding amongst the public about what they should expect, or demand, from the products and services they buy.

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

Such an increased consumer focus should benefit these companies, as they should achieve more business as informed consumers demand better cyber protection. Those businesses that are visibly meeting an appropriate level of service will not only attract more public interest, they will also attract more cyber security professionals wanting to work for them. Government contracts need to be more specific in mandating sovereign capability, maintaining the IP of companies and processing of data to remain in Australia.

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

Consider successful campaigns in the health sector such as HIV awareness and dangers of smoking, as well as campaigns to educate children about road safety and safe houses. The success of these campaigns is measurable as they led to measurably less people being affected by the subject matter at the heart of the campaign. All good campaigns need to have simple understandable messages and they need to be measurable. A good cyber security best practice behaviour change campaign should lead to less people being affected by some of the most common forms of cyber security scams and threats.

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

Yes, it is important that in the very least cyber security features are made known to consumers and this should lead to consumers demanding they be prioritised. This should also have a positive effect on the providers of cyber security products and services from a reputational perspective as public trust in those products increases.

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

Much of the focus of efforts from Government in past years has been on the traditional information environment of networks and desktop computers. More attention needs to be provided to the future environment, in which mobility, non-traditional IoT applications and operational technologies become more prevalent and important cyber security considerations in our society. Some emphasis should be given to how Government will identify those providers of cyber security and operational technologies security products and services to increase public trust in the resilience and safety of Australia's networks.

SAPIEN