OCSC
Oceania Cyber Security Centre

Comments on the Discussion Paper
Australia's 2020 Cyber Security Strategy – A call for views

Submission from the Oceania Cyber Security Centre

Prepared by Carsten Rudolph – [redacted]
Associate Professor for Cyber Security, Monash University
Director of the Oceania Cyber Security Centre

Endorsed by the Chair and Board of the Oceania Cyber Security Centre

Introduction

The Oceania Cyber Security Centre (OCSC) is a collaboration between 8 Victorian Universities and the State Government of Victoria. The Centre provides a platform for industry-led cyber security research in addition to delivering the Oxford University Cyber Maturity Model for Nations in the Pacific region.

This submission focuses on key elements which impact upon effective cyber security policy and program delivery, responsive to issues raised in the discussion paper. The submission is not exhaustive as OCSC has highlighted areas of most urgency, and which the Centre has established capability to effectively assist the Government with its policy agenda.

Developing secure systems

The discussion paper seems to assume that vulnerable systems are the default status and this status is too difficult to change. It is a symptom of accepting defeat, rather than a pathway to long-term improvements in cyber security. Further, this restricted view prevents the strategy from creating a vision that taps into the existing potential in Australia.
It is not clear why it should not be possible for Australia to play an active role in the development of secure solutions or in turning the (often open source) software that forms the backbone of our digitised economy into more secure components. Australia has confidence to build large-scale assets in the defence sector, but lacks confidence in the public and civil sector, in particular in IT, where there is currently no support for the development of secure solutions.
Current cyber security funding mainly focuses on security controls, authentication mechanisms etc. Investing in the development of secure IT products can have a considerable return on

investment, not only in better security, but also in boosting the Australian IT sector of the economy. It seems to be a core assumption that IT components, larger software products, routers, mobile phones etc. must be acquired from outside Australia. Even worse, there are no clear criteria regarding the security of these products to guide business or consumers when making purchasing decisions.

The effect is that Australia will continue to use insecure products and awareness campaigns will fail to achieve their objectives, as users do not have a choice between secure and less secure solutions. Thus, their behaviours matter less than awareness campaigns suggest.

Currently, secure solutions are limited to niche markets and mainly focused on the defence sector. This is a dangerous strategy, as many aspects of social life, economy and critical infrastructure rely on weak and insecure foundations that are difficult or impossible to defend.

We should not consider cyber security to be a "sector" within the IT market and as "features" of a product or service. One example is that there should be no vulnerabilities in software and a product should not enable malicious actors to interfere. One recent example of the problem of accepting the status quo, is Android's NFC functionality that enabled uncontrolled installation of third-party apps from unknown sources. This is an example of a fundamental design flaw. Attacks based on this type of issues cannot be prevented by good user behaviour or additional security controls.

Proposal

The government's strategy should focus on the potential of Australian researchers and industry to develop secure solutions. This should happen in collaboration with local and international technology companies to ensure that these solutions work in the interplay with other solutions. While this is definitely not a short-term solution, there are various aspects that can be achieved step-by-step:

- Debug open source software that forms the backbone of our networks and IT (vulnerability testing, fuzzing, code reviews, etc.; Australian researchers are world-class in this area)
- Build secure-by-design systems. Use cryptography, where suitable, build on trusted components, enable attestation, etc.
- Regulation needs to require secure solutions. This might mean a reduction in complexity and functionality for systems in all critical areas (not only on a national level, but for companies of all sizes and for each individual).
- Strategic investment into developing a core of secure IT products and services.

OCSC
Oceania Cyber Security Centre

Awareness, education and training

The current discussion on cyber security education currently distinguishes mainly two groups. First, cyber security experts in a number of roles and second, the general public that has no particular role in cyber security. In both areas, Australia has made considerable progress through specialised degrees in tertiary education, vocational programs, awareness campaigns, etc. However, there is no doubt that additional efforts are necessary. So far, development was often driven by investment of Universities themselves, and investment of State Governments through sponsored TAFE courses. Initiatives, like the Academic Centres of Cyber Security Excellence are very small and have limited impact, being restricted to two Universities. Collaboration is not encouraged and existing attempts to foster collaboration (e.g. through the NSW Cyber Security Network or the Victorian OCSC) do receive limited or no federal funding.

A few essential aspects are not currently covered by the discussion paper. First, cyber security education and training needs to be seen across all different sectors including IT, agriculture, health, mining, transport, critical infrastructures, communication, architecture, retail, hospitality, just to mention a few. Every software developer needs to understand the pitfalls of software development to be able to create secure code and use tools supporting the prevention of vulnerabilities. Doctors and nurses must understand the risks involved in the systems used in a hospital. Farmers need to recognise that their automated weed control system still works as expected. A long-term strategy and considerable investment is required to advance Australia's education system to be able to cope with these challenges. Universities are already active to push cyber security into other areas, but more effort is required. Second, in training and awareness we need to acknowledge that while behaviour changes can stop some scams and attacks, the choice between right and wrong behaviour is limited and our systems often contradict the message of awareness campaigns. Therefore, awareness campaigns need to properly reflect current systems and processes. Finally, education and training needs to shift from a "strong cyber defences" paradigm to establishing proper risk evaluation and bringing sufficiently secure systems in place.

Door 34, Goods Shed, Village Street, Docklands VIC 3008
E: info@ocsc.com.au **W:** www.ocsc.com.au

OCSC
Oceania Cyber Security Centre

Proposal

Work with education providers on all levels to turn cyber security from a rather specialised topic to *cyber security literacy* as a core competency that is important in all sectors and for all positions. This will require educational research to determine what are adequate levels of cyber security literacy and develop content to support their development. To achieve this goal, the focus will not be on creating cyber security roles, but on injecting cyber security knowledge at the right place where it matters most.

Change the accreditation of cyber security degrees from ACS to another body that understands the needs of cyber security education. While core aspects of cyber security belong to computer science, a very large part goes across many sectors.

Furthermore introduce the element of risk mitigation around the concept of cyber security in other educational disciplines. As discussed, risk in inherent in all vocations and the management of digital and information systems is no different. However every vocation is now accountable for data and the management of sensitive and personal information and accordingly security of such systems should be a paramount focus.

Door 34, Goods Shed, Village Street, Docklands VIC 3008
E: info@ocsc.com.au **W:** www.ocsc.com.au

OCSC
Oceania Cyber Security Centre

International strategy

The discussion paper reflects a rather nationalistic view on cyber security. Australia needs to see itself as a strong partner in the Asia Pacific region which takes on international responsibilities for a secure and open Internet. Many countries in the region move towards digital development. This brings additional risks in the direct neighbourhood of Australia. Therefore, the strategy should reflect the role Australia wants to play. Is it the country that defends itself or do we support our partners in Asia and the Pacific to enable better cyber security across the region? So far, the impact of Australia's International Cyber Engagement strategy has been limited. The strategy was implemented through a number of unsynchronised and ad-hoc activities. The impact can be expected to be much higher with a synchronised approach involving Australian players (e.g. Universities, the Oceania Cyber Security Centre (OCSC), Australian Strategic Policy Institute (ASPI), etc.) international entities (e.g. APNIC, GFCE, UN, World Bank, Asian Development Bank) and other countries (e.g. United States and New Zealand).

Another aspect that should be critically revised is the offensive aspect of the strategy. The idea, that Australia will be able to build up offensive cyber security capabilities that are exclusive to the Australian Government is most probably an illusion. The current WhatsApp example shows that maintaining vulnerabilities in software is a dangerous game. The strategy needs to reflect the international character of the Internet and systems, computers, operating systems, devices, software we use.

The Discussion Paper references that Australia and the the International Strategy has a focus to "build cyber capacity in the Indo-Pacific region and globally, through public-private partnerships". The Paper further notes that an additional $34m is to be invested to strengthen cyber capacity and resilience in the region.

It is difficult at this stage to identify how and where this investment has been and is to be made. The OCSC for example delivers the Oxford University Cyber Maturity Model (CMM) for Nations in the Pacific region. This comprehensive assessment of a nation's whole of cyber security maturity and responsiveness provides an evidence basis for further capacity building initiatives. International agencies including The World Bank and other '5-eyes' nations have used the findings of the CMM as the basis for funding infrastructure and governance/policy improvement programs, however it remains unknown the Australian government's program delivery or focus.

Door 34, Goods Shed, Village Street, Docklands VIC 3008
E: info@ocsc.com.au **W:** www.ocsc.com.au

With established evidence-delivering assessments such as the CMM already active in the Indo-Pacific region, there is no requirement to duplicate existing capability. The Government's response should be to partner with NGOs including the OCSC and use their domestic and international expertise to identify critical vulnerabilities and deliver essential capacity-building programs accordingly.

Proposal

The strategy should create a pathway for Australia to collaborate with its established domestic and international partners to play a supportive role and consider the big picture of an interconnected community. This would also decrease the risk of other countries in the region being used as stepping stones to run cyber-attacks on Australian targets.

The offensive element of the strategy should be critically revised in collaboration with experts from academia. The current proposal seems to be unrealistic and has the potential to be harmful to Australia's cyber security.

Established expertise exists and the Strategy should avoid unnecessary duplication of this existing, underutilised resource.

Door 34, Goods Shed, Village Street, Docklands VIC 3008
E: info@ocsc.com.au **W:** www.ocsc.com.au

OCSC
Oceania Cyber Security Centre

What specific market incentives or regulatory changes should Government consider?

The Discussion Paper does not reference the uptake of Australia's R&D tax incentive relevant to cyber security research. There does appear to be limitation in the current CRC and industry growth centre funding models as the treatment of intellectual property emanating from any collaborative research activities does not appear to be in the interest of a participating industry partner, and the involvement of industry-led research is restrictive to the Centre's prescribed areas.

This limits the opportunity for true industry-led research as an industry partner normally would not want to involve itself with a research project for no gain. This was the limitation of the former NICTA model which ultimately led to its demise.

A more effective system is for a platform approach to industry cooperative research. Industry will have more comfort in working with a 'collaborator' to match research expertise to their specific cyber security challenge. A simple co-funded, equitable grants program administer through a 'collaborator' type program (such as the OCSC) is more cost and process effective than prescriptive terms set by the CRC or growth centre initiatives.

This model is increasingly being used successfully internationally and provide significant economies of scale as well as more effective program and research administration due to industry identifying their problems whilst an independent third party "collaborator" matches the required research expertise and independently manages and oversees the research output.

Again there is no requirement under the new strategy to duplicate established systems and State Governments have initiated successful delivery models which should be expanded and supported under the new Federal Strategy.

Door 34, Goods Shed, Village Street, Docklands VIC 3008
E: info@ocsc.com.au **W:** www.ocsc.com.au