Advisory Board Consolidated Feedback Report

Date:	16th October 2019
Paper:	Department of Home Affairs: Australia's 2020 Cyber Security Strategy – A Call for Views
Board/Committee(s):	Cyber Security Committee

Specific Feedback:

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

   As evidenced by the reported cyber-attack on the Australian National University[1], the threat environment has radically changed over the last 24 months in at least five dimensions, namely:

   - Targeted information systems, consisting of associated server and workstations systems as well as the connecting data network (Internet) itself,
   - The level of sophistication involved, again as evidenced by the reported ANU attack, has rapidly developed to highly detailed, technically sophisticated and expert levels,
   - The spread of those involved has likewise expanded from individual "actors" to "nation state" entities,
   - Almost universal adoption of low security "web-based" services at both enterprise and individual levels coupled with low security computer structures, e.g. the "Android" operating system used in mobile phones / tablets, and an essential monoculture in server/client environments based around a single USA based supplier, Microsoft Inc. rendering that system a "honeypot" for cyber-attack, and
   - Extrajudicial direction, interference has increased and that can't be mitigated purely by technical controls

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

   The current situation is unbalanced with too much responsibility wrongly allocated to the end-user. As pointed out in 2003 at a "Computing Research Association (CRA) – USA- Grand Challenges" meeting, end-users need cybersecurity mechanisms and services they can clearly "understand and manage". This is not the current situation. Moreover, there is general political agreement internationally that "cybersecurity is national security".

   In the "real world" citizens depend upon appropriate government legislative instruments and standards to provide a safe

[1] https://www.anu.edu.au/news/all-news/data-breach

environment, e.g. the Motor Vehicle Standards Act covering what is required of a motor vehicle to be operated on the "open road". Thus, it is imperative that the current massive cybersecurity imbalance be remedied by transfer of responsibility in relation to cyber risk "into industry and business" by provision of appropriate enforced and assessed mechanisms and services, particularly to the IT systems supply industry itself, as in other sectors to the economy.

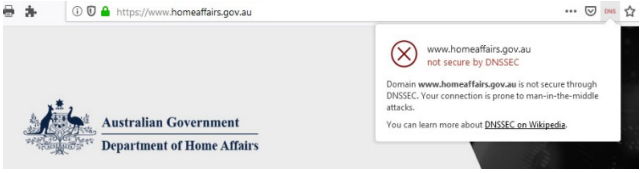
3. **Do you think the way these responsibilities are currently allocated is right? What changes should we consider?**

   The current allocation is not right and needs to be urgently remedied against heightened threats. Given examples of massive cyber breaches internationally over the last 24 months, governments at all levels, Federal/State/Local, need to provide urgent leadership in the "hardening" of information/data server systems based around the internationally agreed "Common Criteria – IS15408" security specifications, profiles and evaluations.

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

   The public sector should take a leading role in *hardening* its own information structures, particularly where these are accessible by the public and thus by any Internet based connection.

   Example: Federal Government internet "domain names" should be readily able to be authenticated using any email/browser check function for DNSSEC conformance. The current situation is given below as an example of the problem. (Site scan at 7 October 2019)



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

   This clause seems to request broad comments on such legislative instruments as the "TOLA" and thus on the use and management of cryptography in relation to privacy and integrity of Federal Government information systems and associated perception by the public, as one major aspect of concern. This has been a problem in public policy terms for well over 25 years as evidenced by the USA's "Clipper Chip" and "Key Escrow" debate of the early-mid 1990s.

Trust involves openness, understanding and commitment by both parties. However, in the case of cybersecurity, the domain of discourse is highly unbalanced.

The government could use Australia's professional societies as a vehicle to provide appropriate levels of education and discourse in this matter in areas related to that profession or enterprise group, e.g. a combination of the Australian Computer Society and the Australian Medical Association, the Australian Institution of Engineers, etc.

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

In simple terms, and as common in other arenas, the product or service offered must be suitable for use in the designated environment which means connection to the global Internet.

As in the motor vehicle example above, the cyber product offered must be suitable for its intended and marketed usage without necessary addition of supposedly essential protection sub-systems, just as buying a car is understood to include its seat-belts.

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

As for 6. above, government can mandate basic security facilities be incorporated into products and systems offered by vendors for use by the public sector.

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

In the 1990s the United States Government introduced a "C2 by '92" and even, later, a "B2 by '95" cybersecurity purchasing mandate for all Federal systems in that country, This had an immediate affect in such companies as Microsoft, with its "Windows NT Ver 4.0" enhanced "Discretionary Access Control (DAC)" profile and attempted TCSEC "C2" evaluation. While this assisted markedly in getting security attention at this level, as distinct from the computer mainframe systems of the time, it was not wholly successful as even the USA's public sector claimed problems with increased costs and expertise eventually rendering the program largely unsuccessful.

Today, a major step forward could be done through mandatory government purchase specifications detailing enhanced security features and evaluation for nationally significant servers systems, e.g. RedHat Enterprise LINUX Vers 8 with "AppArmor" / SELinux profile as per the detailed "Essential 8"[2] from the ACSC.

[2] https://www.cyber.gov.au/publications/essential-eight-in-linux-environments

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

   There is no evidence that cybersecurity has ever been a major concern of the private sector or of the basic ICT industry itself as evidenced by the massive growth of a separate cybersecurity "add-on" industry worldwide. The very existence of the "Common Criteria" for evaluation of cybersecurity products and systems demonstrates the fact that the IT industry itself never progressed to full industry level security compliance. Like other safety and security areas, from policing to aviation security, the primary motivations of government and the private sector are different. An example of this would be likening it to the privatisation of the Australian Federal Policy Force or sections of the Army, Navy or Airforce.

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

    The regulatory regime, particularly for owners and operators of national critical infrastructure systems and similar vitally important sectors such as healthcare, education, etc. is not appropriate at present as evidenced by the successful attack reports given in this paper and the accelerating attack expertise evidenced by recent events potentially involving nation state entities.

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

    Government should re-examine the motivation for the abandoned "B2 by '95" suggestion for government ICT systems procurement in the USA. Essentially, in combination with Australia's allies, particularly the "5-Eyes" group, procurement of particularly server systems with the minimum eight, particularly the recommended "AppArmor/SELinux" subsystem set, must be mandated with phase-in over the next 18 months at the outside.

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

    There are two options:

    - The legal/regulatory environment makes cybersecurity a mandatory feature of both public and private sector information systems development, procurement and operation, or

    - There is sufficient exposure by the public to significant data/information system breaches, denial-of-service,

ransom threats and the like that the marketplace comes into operation for more secure systems. Note this would be a very long term solution and has shown few results over the last 30 years or so. For example, there is general agreement that the Internet was created and expanded with little to no emphasis on security.

Recently Hyppönen, addressing an a security forum in Sydney told CIO Australia: *"the internet - with 2.4 billion users - was never designed to be a secure system. The internet was designed to be an open and fault-tolerant system."*[3]

13. **How could we approach instilling better trust in ICT supply chains?**
    As an "ICT colony", without an indigenous ICT product and system industry, as distinct from an ICT system application developer and marketer, independent and published evaluation is needed as to the security posture of imported products and systems, as well as their supply chain, in much the same way as happens with many other products, e.g. through the "Choice" group. The recent Australian Government stance on incorporation of Huawei 5G products into Australia's 5G mobile telecommunications network illustrates that need as it applies to all Australian enterprises and not just critical infrastructure owners and operators or the public sector.

14. **How can Australian governments and private entities build a market of high-quality cyber security professionals in Australia?**
    The experience of both the USA and UK in the development of desperately needed cybersecurity professionals give a ready indication of steps needed. The USA's "Centers of Academic Excellence (CAE)"[4] and the UK's "Academic Centres of Excellence (ACE)"[5] programs need to be quickly assessed and emulated. Where these programs involve compulsory employment "bonding" of scholarship recipients, such requirements should not be shunned.

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

16. **How can high-volume, low-sophistication malicious activity targeting Australia be reduced?**
    It mostly cannot be reduced in the short to medium term. However, given that such activity appears to be largely of

[3] https://www.cio.com.au/article/569270/internet-designed-security-warns-international-expert/

[4] **https://www.nsa.gov/resources/students-educators/centers-academic-excellence/**

[5] **https://epsrc.ukri.org/research/centres/acecybersecurity/**

overseas origin international, government-to-government meetings and agreements on this topic could assist.

17. **What changes can Government make to create a hostile environment for malicious cyber actors?**
Australia has already noted its development of cyber-operations capacity in both intelligence and defence arenas. As mentioned in reply to 14. Above development of the appropriate cyber-operations education and training programs in Australia would assist in line with the USA's "CAE-CO" program, for example.

18. **How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?**
The two basic remedial actions are:
    - Enhanced training and education in cybersecurity to develop Australia's notably under-developed cybersecurity professional cohort. This includes examination of the need for "educate-the-educator" and "train-the-trainer" programs to enhance the supply of suitable teachers and researchers in this area at both university and TAFE levels; and
    - Concrete and specific advice and recommendations from relevant government and academic entities through subsidized support for appropriate analysis and consultancy activities.

19. **What private networks should be considered critical systems that need stronger cyber defences?**
Beyond the usually accepted national critical infrastructures, such as power, water, etc. both healthcare and education systems need to be considered "critical systems" in that they maintain sensitive personal details of interest to cyber-attack entities. At the same time, food distribution needs to be considered given the nature of the Australian landscape and dependence for food delivery by major centres of population particularly the State capitals.

20. **What funding models should Government explore for any additional protections provided to the community?**
In particular, Australia's TAFE structures could be funded to provide necessary and sufficient awareness and education programs for the general public.

21. **What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?**
Simplified security "clearances" for this particular purpose could be considered on both permanent and temporary/as needed bases.

22. **To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?**
Consumer choice has to be viewed against market reality. Microsoft Inc. and Apple, Inc., USA, based systems have been labelled, in other domains particularly including the small-to-medium business level as well as the consumer environment, as essentially comprising an international monopoly. In this sense "market offerings", and thus choice, are severely limited if not non-existent.
Choice may exist with a wide variety of "add-in" cybersecurity sub-systems available from a number of countries besides the two major countries of the USA and UK. The question will take on new complexity dimensions for the consumer as China enters the marketplace for basic IT hardware and system software.

23. **How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?**
The add-in cybersecurity product area is a hugely contested and international marketplace with large scale government level support for product and systems development and marketing by such nations as Israel, USA, etc. While enhanced "consumer focus" is always beneficial it may have little to no affect at all on an indigenous market in this area without new and markedly increased venture capital for the sector coupled with aggressive public sector purchasing of indigenous products and services. Increased awareness may just do the opposite and increase importation of overseas supported products and services.

Finance for this arena is vital and of large scale overseas, by Australian standards. A USA 2018 report, for example, states as follows:

- "The market for cybersecurity venture capital was strong in Q2 2018. Both deal volume and deal valuation were high. For example, in June, BitSight Technologies raised $60 million in financing, Agari announced $40 million in funding, and Claroty raised $60 million. In May, Signifyd saw $100 million in funding and IronNet raised $78 million. In April, Saviynt raised $40 million and BetterCloud secured $60 million in financing."[6]

This is repeated for Q3 2019 as follows:

- "It was a strong quarter (Q3 2019) for the cybersecurity market in terms of deal volume and deal value.The quarter started out strong with SoftBank Group Corp.'s $200 million investment in Cybereason. In August, deal volume lagged slightly, but deal value did not: OneTrust closed a $200 million Series A investment round led by Insight Partners. In September there were no deals that

[6] https://cybersecurityventures.com/vc-report-list-of-cybersecurity-companies-that-raised-venture-capital-in-q2-2018/

hit the $200 million mark. However, deal volume picked up, leaving a promising outlook for the year's final quarter."[7]

This same US firm has also made the following comments and predictions:

- "In 2004, the global cybersecurity market was worth $3.5 billion — and in 2017 it was expected to be worth more than $120 billion. The cybersecurity market grew by roughly 35X over 13 years entering our most recent prediction cycle. Cybersecurity Ventures predicts global spending on cybersecurity products and services will exceed $1 trillion cumulatively over the five-year period from 2017 to 2021."[8]

  This report sees USA Federal Government expenditure on cybersecurity as a MAJOR influence on the marketplace, including the reported USA Presidential budget of "..$15 billion for cybersecurity.."

  Summary: While consumer enthusiasm for cybersecurity products and services is to be welcomed, without the necessary government support and incentives coupled with appropriate venture capital, at the levels needed to enter the global marketplace in this area, such increased consumer awareness may be of little use to development of an indigenous industry at any level necessary to compete globally.

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

25. **Would you like to see cyber security features prioritised in products and services?**
    Cybersecurity features need to be specified as mandatory, and not just given priority, in procurement documents for public sector procurements at all levels, from mobile phone to tablets to laptops to desktops to servers to network components, etc.

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

    - In terms of a strategy, you need to secure your key assets first. This provides confidence throughout the community and lifts expectations of supply chains. Regulation considerations need to be assessed for critical infrastructure. While raising the cost base of providers, it does do so equitably, with the flow on effects of

[7] https://cybersecurityventures.com/q4-2019-vc-report-cybersecurity-venture-capital-investments-in-the-latest-quarter/

[8] https://cybersecurityventures.com/cybersecurity-market-report/

providing greater consistency in addressing cyber risk and lifting confidence.

- To provide differentiated products and services higher up the value chain in a digital economy, there is a critical role for sovereign cyber innovation to support the achievement of Government's objectives on national security as well as the cyber maturity of the economy and community.

- To ensure a world Australian Cyber professional and Australian Cyber Industry, regulation and legislation needs to be balanced recognising the playing field elsewhere in the world, and where possible, co-designed. Given the pervasiveness of the digital economy and digitisation trends, there is a need to run a cyber lens across all policy development to achieve security by design.

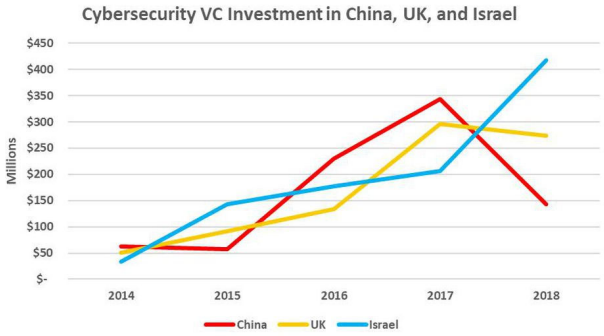
- Education: The critical element in these considerations is the reported dearth of cybersecurity professionals in Australia capable of providing the necessary management levels needed to safeguard the cyber-environment. An education and training program along the lines of the USA's CAE and the UK's ACE programs is required as a major matter of urgency. The most expeditious strategy to infiltrate the education system is through plug and play resources so that teachers can adopt who have not necessarily the trained background in technology and cyber.

- Venture Capital: To participate in the global cybersecurity "add-in" marketplace Australia needs a venture capital market in rough alignment with those other countries who have entered the field, e.g. Israel, etc. Specific public sector "buy local" programs have a major part to play in the development of the sector and any associated venture capital and financing market.

  The Israel example is enlightening as follows: "In 2018, Israeli start-ups received $1.19 billion or almost 20% of global VC investments in cybersecurity, up 47% from the previous year, according to a new report from Start-Up Nation Central. Another report, published by Strategic Cyber Ventures, shows that Israel has surpassed China last year as the hottest spot for VC investments in cybersecurity companies outside of the US."[9]

  The investment graph from the above report show additional investment in the sector in China, as follows.

[9] https://www.forbes.com/sites/gilpress/2019/02/26/israeli-startups-shine-in-the-92-billion-cybersecurity-market/#5d738d5d451d



Submission Prepared By: Marc Portlock – Strategic Initiatives Executive TAB