Australia's 2020 Cyber Security Strategy

Responses by John Moushall

Question 1

What is your view of the cyber threat environment?

Personal Identity theft is a major issue with most people completely ignorant of small actions that can be taken to preserve their safety, such as putting a lock on their letter box.

Businesses, large and small, do not take the APPs seriously. That is, poor control of PII through emails and their operations. A lack of ICT systems security and monitoring in place to manage privacy. This is strongly coupled with poor staff awareness of ICT security including email phishing, spear phishing, confidential data handling and security of records.

There are a large number of IT service providers which businesses increasingly rely on for outsource general IT and IT cyber security. Very few, if any, seem to have any formal qualification of their systems management or an ISMS, for example ISO27001, COBIT, ITIL. Yet these companies manage a large portion of Australian businesses IT including SMEs seeking professional guidance. Getting to the root causes of poor practises in the IT supply services sector would have a broader effect than attempting to go to every user. Put responsibility back onto the supply chain.

Of the twenty-five top ICT providers in Australia[1] none advertise, or appear to have, any compliance to IT or IT cyber security standards.

Reputational loss and impact. The Landmark White data breach is an example of the devastation of the business and job losses that occur.

What threats should Government be focusing on?

With the rapidly changing landscape, it is impossible to cover everything.
The main three are:

a) A stronger set of controls on IT service providers supplying ICT and Cyber security for example, meeting international standards for IT and ISMS, proven compliance to standards.

b) Identity theft is often low tech for example phishing, yet it contributes to a large portion of crime and has severe long terms impacts on people and their families.

c) Ransomware needs to continue to be addressed due to the large growth in attacks and low technical skills, resulting in devastating consequences for individuals and small businesses.

[1] Top Managed (IT)Service Providers in Australia, Cloud tango, Accessed 9 September 19, https://www.cloudtango.org/topMSPs/AU/

Responses by John Moushall

Question 2

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

Yes. The responsibility for cyber risk should be passed along the whole supply chain including the end users. This is no different to workplace health and safety requirements to protect people from unnecessary physical injury including an individual's responsibilities and similar to the fiscal control practises through APRA to force proper financial due diligence.

Question 3

Do you think the way these responsibilities are currently allocated is right?

<u>General Business and PII</u>

A. No. There is not enough control on general business to manage these critical functions. For instance, the banks only appeared to take notice of their obligations along the supply chain with the introduction of CPS 234.

   Similar discussion should be had along all supply chains that are handling PII. Not just those above $3M turnover.

   Large businesses seem to place more emphasis on marketing information / mining customer data than the PII. After testing a number of large public companies on their Privacy management by making application, only one in eight passed some of the basic requirements. The companies tested were Australian Super, Australia Pacific Airports (Melbourne), BUPA, Gippsland Water, Internode, Telstra, and Western Union.

   The major areas of failure for PII enquiries were:

   a) Sending (Gippsland Water) or requesting (BUPA) sensitive personal information such as date of birth, driver's license numbers and account numbers over open email;

   b) no clear privacy management process despite having a Privacy policy;

   c) forcing individuals to abrpogate their PII rights to use services by agreeing to the Privacy policy to enjoy the services (APA);

   d) "Bullying" by the large public companies by quoting legislation, often misleading, and attempting to intimidate the enquirer;

   e) inability to identify data held – If it cannot be found how can it be protected?

f) deliberate delays and barriers to supplying information;

g) recording all telephone calls without initial consent of the caller. When questioned there no management systems, or realisation of, digital voice recordings as sensitive data; and

h) no apparent concern over complaints to the OAIC – Currently the OAIC is thirteen months behind on privacy complaints[2] from the public.

<u>ISP, IT Service and Cyber Security Providers</u>

B. No. There is not enough control on IT service and Cyber security providers that purport to deliver essential cyber and IT infrastructure services.

These are actual documented major areas of failure for IT Services and Cyber Security providers:

a) Setting up firewalls and other sensitive devices with default configuration often leaving the User ID and/or Password at device defaults;

b) Failing to monitor firmware, OS, AV and malware patching. Patching up to 15 months out of date;

c) Failing to blacklist devices before placing them on a network and then open ports as required;

d) Poor/No management of the Active Directory services often leaving employees with access rights in the system months after they have left an organisation;

e) Failing to secure telephony through the firewalls resulting in call cost losses from IP spoofing; and

f) Providing penetration testing from professionally unqualified staff, using online tools for a 2-minute test and charging exorbitant rates in thousands to small businesses;

[2] Email from Kate Thorpe, Investigations Officer OIAC, 7-8-19 "OAIC is just commencing complaints from September 2018"

Responses by John Moushall

What changes should we consider?

a) Increased legislated data management and security of all personal data under the APPs for all businesses;

b) Legislative management of IT Services and Cyber Security providers to minimum levels of security management. This is similar to the banks under APRA prudential standard CPS 234 especially by placing responsibility on the boards for compliance and specifying the operational controls of these businesses;

c) Providing a free inspection service to SMEs. A one-day audit of their actual operational processes and a vulnerability scan of their systems. 70% of data breaches occur from human factors, accidental or malicious.[3]

d) Public education campaigns at school level as part of the curriculum and in media. More educational emphasis with advertising campaigns like the road toll and smoking "shock" ads, on the personal price of identity theft.

Question 4

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

Consideration should be given to providing immediate mitigation advice and help when a data breach is identified. This would assist government to capture more of these events for metrics and investigation. From there on businesses will have to manage their own forensic investigation, equipment replacement, breach notification, media releases and getting back into operation.

Question 5

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

Unfortunately, even the government is not beyond hacking, so this raises a level of distrust.

Any government of the day will not have the trust of the people unless they are prepared to legislate to protect the integrity of the information provided by businesses and ordinary people. This is clearly displayed by the distrust of the My Health Records (MHR) Act. People do not want their information given for one purpose to be "loosely available" to other government departments, agencies or the public. MHR exacerbated the distrust by being an opt out system and not opt in. No one likes government telling them they must give up their privacy rights, no matter how well intentioned.

[3] Connolly, Byron, 2019, CIO, The phishing issue: Michael Connery demonstrates, Accessed 14 September 19, https://www.cio.com.au/article/656560/phishing-issue-michael-connory-demonstrates-how-vulnerable-really/

Trust has to be earned. If the government sees these issues as serious, and there is no doubt they do, then until there is clear legislation that cannot be easily overturned regarding information provided for one purpose not being used for another, there will be no trust.

Question 6

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

As responded to in question 3 B. Companies that are providing IT service and Cyber security need to be legislated to a minimum standard. Cyber security threats rate with Workplace Health and Safety, and Environmental controls.

Question 7

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

Continue to work closely in the JCSC programs working to improve IT standards and drive building security into IoT products.

Question 8

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

Response at 3.B.a, Legislative management of IT Services and Cyber Security providers to minimum levels of security management. This is similar to the banks under APRA prudential standard CPS 234 especially the placing responsibility on the boards for compliance and specifying the operational controls of these businesses. These businesses are not doing it now and need to ne held accountable as they provide services across multiple industries.

Controlling the service providers behaviour is more cost effective than dealing with the thousands of end users.

These are actual documented major areas of failure for IT Services and Cyber Security providers:

a) Setting up firewalls and other sensitive devices with default configuration and in some cases, leaving the User ID and/or Password at device defaults;

b) Failing to monitor firmware, OS, AV and malware patching. Patching up to 15 months out of date;

c) Failing to blacklist devices before placing them on a network and then open ports as required;

d) Poor/No management of the Active Directory services often leaving employees with access rights in the system months after they have left;

e) Failing to secure telephony through the firewalls resulting in call cost losses from IP spoofing; and

f) Providing penetration testing from professionally unqualified staff, using online tools for a 2-minute test and charging exorbitant rates in thousands to small businesses;

Question 9

Are there functions the Government currently performs that could be safely devolved to the private sector?

SME system risk assessments for both infrastructure, cyber security and process weaknesses in their business. This could be subsidised by government.

What would the effect(s) be?

High take up of the offer for a free threat review which they generally cannot afford and a higher level of trust with commercial arrangements in place for confidentiality.

Question 10

Is the regulatory environment for cyber security appropriate?

In short, no.

Why or why not?

As responded to in earlier questions, there is not enough control on ISPs or IT service and Cyber security providers that purport to deliver essential internet, cyber and IT infrastructure services.

Question 11

What specific market incentives or regulatory changes should Government consider?

Offer SME system risk assessments for both infrastructure, cyber security and process weaknesses in their business. This could be subsidised by government.

Provide legislative management of ISPs, IT Services and Cyber Security providers to minimum levels of security management. This is similar to the banks under APRA prudential standard CPS 234 especially by placing responsibility on the boards for compliance and specifying the operational controls of these businesses.

Of the twenty-five top ICT providers in Australia[4] none advertise, or appear to have, any compliance to IT or IT cyber security standards.

Question 12

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

Most network devices inherently obey network rules in order to operate on a network including visibility, be agent managed and capable of security control. So for computers routers, modems and other devices this is already in place by design

Whereas IoT are designed inherently for connection ease first and security second, if at all.

I doubt that it is physically possible to control or monitor building of cyber security into all things IoT.

IoT are generally agentless, therefore effort should be given to network solutions that have an Agentless IoT option. For, example how can a business put an agent on the device a courier brings into the workplace to scan package deliveries?

Secondly, the growth rate in IoT devices would outstrip any management controls put on individual IoT goods.

There are in thousands of IoT items already in Australian households today like Smart TVs, watches, projectors, printers, HVAC and even medical devices that were not designed for an agent or with network security in mind.

To be effective, an IoT security solution needs to see devices that may be "off" the approved or managed network. Therefore, working on an IoT security solution should be a priority and this solution should then become a product requirement in firewalls and routers. Only with the data requirements listed below as an example, can a network solution assess the policy compliance or posture of a specific device.

Some examples of IoT products readable data:

- Profile and fingerprint any device
- Determine the state of that device
- Attack surface posture
- PCI/HIPAA compliance
- Jailbroken status
- Vulnerability history
- Number of wireless protocols
- User authentication
- Manufacturer reputation
- Track the device behaviour and connections

[4] Top Managed (IT)Service Providers in Australia, Cloud tango, Accessed 9 September 19, https://www.cloudtango.org/topMSPs/AU/

- Provide historical record of the device behaviour
- Associate devices with approved users

Question 13

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

The old adage springs to mind. “A chain is only as strong as its weakest link”.
A review of the delivery supply chain for Internet, IT service and cyber services where the industry controls and the on selling of service and equipment is poorly controlled.

For example,

ISPs - mandating ISPs provide AV, malware, SPAM filtering and VPN capabilities for their users – both private and commercial as a standard package. Ensure Modems / routers contain unique ID and password configurations and not device defaults. This is doen by some ISPs but not all.

IT Providers - are largely MSPs that outsource by buying wholesale service offerings with little or no management of the sourced product to the end user. There is often a very large knowledge gap between the MSP and the product or services they are on selling. The IT wholesalers should be responsible to ensure the MSP services being provided are by reputable and qualified technicians. Microsoft has a very good system for making resellers achieve product knowledge. Unfortunately, this is not the same across the industry for products and services.

The need for MSP education is important as it is the MSPs that are left configuring the goods and services for the end user. See response in 3B. for areas of concern by IT MSPs in end user cyber safety.

Question 14

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

A. Providing IT Degree places at Universities at not cost to the student contingent on achieving minimum pass grades each year to continue or alternately wiping out HECS debts after graduating and spending 3 years in an IT business in Australia or similar.

B. Offer cadetship programs, similar to trade programs, by subsidising placement of cadets in MSP, government and cyber security companies

IT MSPs are seen as one solution to the growing skills shortage. A cadetship with an IT MSP is a smart solution due to the rapid changes in technology for graduates isolated in an academic environment and the IT MSPs being at the coal face of that rapidly changing environment.

However, there needs to be a lift in the quality of the IT and cyber MSPs as previously discussed in the response.

Question 15

Are there any barriers currently preventing the growth of the cyber insurance market in Australia?

There should be no barriers in Australia to cyber insurance growth although there are concerns that global cyber insurance may collapse[5] if it does not expand scope. All companies need to protect themselves.

Growing Cyber insurance offering involves Insurance providers working more closely with cyber risk companies to leverage user cases, software and hardware vulnerabilities to understand the risk. Current insurance seems to only focus on losses related to digital assets like data breach, cybercrimes and data loss.

Other areas of insurance that do not seem to have been explored involve cyber insurance for business interruption including network and service liability, and risk modelling to develop new products serving untapped areas such as intellectual property (IP) theft insurance.

In addition, cyber insurance could include damage to intangible assets that are not cyber risks, such as reputational harm due to product recall/data loss, which is rarely covered by traditional insurance. An example of this would be the Landmark White (LMW) breaches in February 2019 that have had a severe impact on reputational loss, that is immediate loss of the big four banks work, which has cost more than the confidentiality value/costs of the data lost. LMW have halted trading on the ASX twice, and at the time of writing, do not seem to be recovering seven months on.

If so, how can they be addressed?

Insurers can drive business behaviour where businesses remain slow to implement preventive measures due to low awareness and recognition of the value of such services.

Lower premium incentives raise business desire for implementation of effective controls and move them toward preventative services, and for the insurers, lower risk and claims.

Extending their offering as outlined above would also increase their market and assist with the risk cover spread.

`Question 16

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

[5] Woods, D.W. and Moore, T., 2019, Does Insurance Have A Future In Governing Cybersecurity?, Accepted For Publication In IEEE Security & Privacy, Accessed 9 September 2019, https://tylermoore.utulsa.edu/govins20.pdf

Responses by John Moushall

In the provided document, Cyber Security Strategy, ransomware and identity theft are both low sophistication malicious activities with severe financial and emotional impact in Australia.

Some obvious answers are that we need continued education at schools on cyber security, media campaigns like smoking and the road toll to get the message across, and it should remain topical by media updates.

The high volume, low technology is aimed at the masses and the best short solution is continual awareness.

Question 17

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

Improve counter cyber activities of reactive strategies, look for predicative algorithms to insert into network environments proactively detecting change. Continue to publicise state owned asset attacks and keep political pressure/reprisal on these states.

Question 18

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

Basic 101 systems lockdown - Properly configured firewall and networks, user access control, DLP, implementing and following a cyber security standard like ISO 27001, educating and staff awareness with regular enforcement.

The installation of AI predictive software[6] to monitor network management and detect movements in behaviour. While most people may baulk at this at work, they readily use this with social media and entertainment platforms such as Spotify, Netflix, Face book and YouTube.

This becomes a trust issue with private businesses and government using these systems. In other words, these AI predictive systems need to be regulated with disclosure of personal privacy coupled to punitive actions for releases private data and automatically anonymising data.

Question 19

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

All networks associated with utilities (gas, electricity, water), transport (air, train, bus and road), health (pharmacies, doctors clinics, hospitals, medical services, aged care facilities),

[6] Chen, H.M. Kazman,R Monarch,I and Wang P., 2017, Can Cybersecurity Be Proactive?, Proceedings of the 50th Hawaii International Conference on System Sciences, Accessed on 14 September 2019, https://core.ac.uk/download/pdf/77240187.pdf

communication (internet, telephony, radio, television), Production (food, petroleum) and financial networks (Banks, ATMs).

Question 20

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

These are contained in previous responses. SME business and infrastructure audits to assist with understanding on what needs to be done by the SMEs. Cadetships for more IT professionals, and early mitigation for cyber-attacks.

Question 21

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

It is a recurring theme, trust. Businesses are driven by commercial constraints and government by "a need to know" to levy taxes and have compliance. It will require some thought about transfer of information to other government agencies not directly connected to the cyber threats and protection of commercial information.

Government unfortunately has a track record of breaking promises when convenient.

Question 22

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

Totally agree. A lack of information about security features and the consequences does not let consumers make the right choice. Buyers exercise their choices generally on features, then cost to get those features without understanding the impacts.

The security features of all IoT device should be built in going forward so that security is no longer a feature or option to have to be considered.

Question 23

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

Increased consumer focus drives innovation and the consumer drive makes the desired attribute a standard feature. Continue to educate the public so that consumer pressure in the form of choice as drives innovation.

Question 24

What are examples of best practice behaviour change campaigns or measures?

There are a number of Interactive programs that simulate phishing attempts for example a good analytical program is from Sopho[7]s, and other individual focussed attacks, so that if a user initiates, the immediate response is a test site explaining what has just happened and runs the user through a training program

How did they achieve scale and how were they evaluated?

These types of programs can be pushed out over small and large enterprises with subsequent responses and training recorded for analysis and follow up with the individuals. These are not meant as a blaming tool but to guide people across the cyber landscape and let them learn by mistakes that are not at the expense of a real breach.

It also provides awareness training usefulness by running these exercises a few weeks after training. These types of tests can be run by the ASD with agreement of private businesses.

This would assist the businesses with their training needs and give the government a much broader statistical threat analysis at the individual level.

Question 25

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

Yes. In addition, Agent programs development should be encouraged to be added to firewalls to identify and manage IoTs currently on the network.

Question 26

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

Clear, consistent and frequent information releases. The JCSC are a great starting initiative.

[7] Sophos Software, 2019, Sophos Phish Threat, Accessed on 9 September 2019, https://www.sophos.com/en-us/products/phish-threat.aspx