UNISYS | Securing Your Tomorrow®

Australia's 2020 Cyber Security Strategy

Unisys submission

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

The cyber threat environment globally and in Australia is increasing rapidly. The risks in the Commercial sectors focus mainly on stealing data for monetary gains. The risks in the public sector are ever increasing with threats from nation state actors with a clear mission to disrupt or compromise target governments, organisations or individuals to gain access to valuable data or intelligence and can create incidents that have international significance. The Government should be focused on any threat that could cause grave damage to the national interest, organisations or individuals. This is supported by the Unisys Cybersecurity Standoff Australia research which states that "52% of CISOs surveyed are concerned about state-sponsored spying and corporate espionage".

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

Unisys does not believe this is well understood. The responsibility for managing cyber risks falls onto everyone involved in the digitally connected economy. This understanding can likely be improved via a targeted outreach education program and establishing recommended and comprehensible baselines for what is an acceptable cyber security standard across the board.

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

Unisys does not think the responsibilities are currently allocated correctly. The changes that are needed is to ensure everyone is aware of their individual responsibilities and how they can meet and ideally exceed those responsibilities. This requires a targeted education program to ensure nationwide cyber resilience and establishing recommended and importantly comprehensible baselines for what is an acceptable cyber security standard.

According to the Unisys Cybersecurity Standoff Australia research "less than half (43 per cent) of Australian organisations surveyed consider cybersecurity to be an integral part of the organisation's strategic plans and objectives. Dig a little deeper and it is clear those at the helm of business, CEOs, predominantly see cybersecurity in tactical terms as either an IT issue (14 per cent), compliance requirement (16 per cent) or a matter for operations to manage (18 per cent). Less than a third (27 per cent) of CEOs view cybersecurity as part of the organisation's business plans. When asked to rank their organisations current business priorities, protecting critical internal data was listed last. Furthermore, the fact that a quarter (25 per cent) of all organisations do not report cybersecurity priorities or concerns to their board shows a dangerous lack of understanding regarding the value of the organisation's data, and the risks and potential liabilities they could face if it were compromised. Reporting appears to be a particular concern among SMEs where just 58

per cent of those with a board report on cybersecurity matters on a regular basis, compared with 72 per cent of government or largescale entities."

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

To assist in awareness of threats and provide assistance as needed to mitigate those threats. This involves an education program, access to threat intelligence information as well as helping ensure that institutions and businesses have access to tools and skills necessary to build their cyber resilience. The Government should also establish baselines of minimum accepted cyber security standards as well as provide relevant regulations and enforcement. Self-regulation with cyber security, simply does not work as businesses don't necessarily see the value in investment.

Unisys suggests a specific budget to be assigned to eligible Small Medium Enterprises (SMEs) to improve their cyber security posture according to the agreed standards. Most SMEs do not utilise agreed and established standards to manage their cyber security posture. According to the Unisys Cybersecurity Standoff Australia research "When asked about how their organisation manages compliance, those in the SME sector are the least likely to believe their approach is based on recognised industry frameworks."

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

The trust can be ensured through transparency on its initiatives and focusing on results. When governments are transparent (as far as feasible) and demonstrate results, trust will follow.

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

Consumers should have confidence and a level of protection that acquired cyber goods (hardware and software) should be suitably tested for major flaws or defects. They must receive supplier commitment there isn't any hidden method that could be used to bypass access authentication without being detected and be guaranteed to work as advertised. The government can assist by setting up a Trusted Vendor program for cyber goods that certifies these as defect free. For cyber services, they need to be provided in a professional and ethical manner and should deliver on the agreed outcomes.

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

Education is key. Access to resources such as DYI tools, support network or hotline and educational material is essential. Government and industry can help provide these resources.

Cyber security is a key concern for Australian citizens. According to the Unisys Security Index, 2019, "The top three security concerns for Australians relate to data theft. 57% of Australians are seriously (extremely/very) concerned about unauthorised access to or misuse of their personal information. 29% of Australian's are aware their data was compromised in the last 12 months."

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

Ensuring quality and security must be factored into the product development lifecycle. Too often both of these are an afterthought and results in insecure or defect products being delivered to market. The Government should establish baselines of minimum accepted cyber security standards as well as provide relevant regulations and consider adopting the role of standard enforcement.

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

Yes. The Government should focus on cyber threats that could have grave effect on national security. All other threats should be analysed and devolved to the private sector with oversight from relevant Government sectors. The results would be a more focused approach to national security as well as the private sector sharing the responsibility with oversight from the Government.

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

No. Very few in the private sector improve cyber security unless they are regulated to do so. At the moment regulations are weak or non-existent in this area. Further, those that do exist (such as the Australian Privacy Principles) are impotent as penalties are either immaterial or not enforced. Regulation should be built around protecting personal information and critical data backed by strong enforcement.

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

We believe that both are required. Those that are proactive around cyber security should be prioritised with preferred supplier status for Government contracts, as an example (incentive). Those that are remiss should attract regulatory pressure and where applicable, penalties applied.

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

Cyber security must be built into the development lifecycle of digital goods and services. Regulation must be implemented and enforced which works to assure cyber safety of digital goods and services with the aim to avoid defected goods being released to market.

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

The supply chain must be documented and understood. Minimum cyber security requirements relevant to the industry sector should be established and considered mandatory for participating organisations. Organisations that are assessed as non-compliant should be excluded from the supply chain. The integrity of the supply chain and those of participating organisations is critical. It

has been well documented malicious actors will target the supply chain (the soft underbelly) with intent to compromise other connecting organisations.

According to the Unisys Cybersecurity Standoff Australia research, "Of those surveyed, SMEs were the most likely to have a reactive approach to managing compliance (30 per cent)". This reactive approach is likely to have a negative impact of the cyber security of SMEs and will eventually affect the entire supply chain.

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

This requires an industry wide approach that includes public and private partnerships to provide the education opportunities (public) and employment opportunities (private) to foster this development. Adopting a combination of opportunities and varying generational employment incentives (i.e. compensation, flexible hours, job security) has an improved chance of attracting and retaining cyber security professionals in country.

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

Yes. The market is in its infancy with many parties navigating their understanding. Insurers are struggling to quantify the risk before underwriting. This can risk clients being underinsured or not covered adequately for the risks they were originally seeking coverage for. This can be addressed by the establishment of a Code of Operations that sets a baseline for risk analysis and mandate a minimum standard for plain English contracts that aids understanding the applicable coverage.

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

Thrill-seekers are typically at the lowest level of sophistication as they often rely on widely available tools that require little technical skill to deploy. Their actions, more often than not, have no lasting effect on their targets beyond reputation.

Governing access to these tools would be impractical, however the observation of malicious activity of those employing these tools isn't and stronger enforcement and penalties must be internationally applied and might work to deter the next thrill-seeker.

Some measures recommended are:

Better education for consumers around phishing attacks in particular

Better implementations of security at the Operating System level by vendors

AI implementation at the ISP or even DNS level to monitor traffic origins and kill/flag suspected traffic such as those going to know Command and Control sites

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

The focus needs to ensure a well-educated and 'armed' offensive capability that immediately demonstrates to adversaries that attempting to compromise a government asset is met with equal or more force to disarm and disable.

Defining policy on attribution and shortening attribution cycles is gaining momentum in public discourse. Attribution is most effective when timely and transparent, driving cyber resilience and trust in our online environment.

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

The Government should be elevated as the trusted source of threat intelligence information to providers of critical infrastructure and aid better understating of the threat landscape and critically guide associated mitigations. Standards must be established ensuring the protection of critical infrastructure.

The Government should also create regulation specific to the cyber security of critical infrastructure backed by strong enforcement and penalties. The Government should pass laws that allow it to audit the cyber systems of critical infrastructure providers and give itself the power to remediate serious flaws in order to prevent mass outages and disruptions to services or threat to human life.

Whilst regulation is a necessary lever in defining the minimum standards necessary for controls on essential and private networks, it is important to avoid a patchwork of intersecting and potentially contradictory contextual regulatory frameworks. It is recommended that government take a proactive approach to coordination of regulatory frameworks from departments and industry bodies to promote a consistent, holistic and economy-wide approach to regulation aimed at protection of essential networks.

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

- Utilities including the power grid, water, sewage
- National and state infrastructure such as roads, airports, ports, etc.
- Banking and finance, telecommunications sectors
- Essential distribution points such as fuel and food
- Chemical and nuclear facilities
- Dams
- Defence facilities
- Emergency services and hospitals

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

Joint public and private partnerships should be explored. Incentives for the private sector could be as simple as brand awareness delivering and supporting these initiatives. Providing additional protection in the form of education and cyber tools is key as according to the Unisys Security Index, 2019, "The top three security concerns for Australians relate to data theft."

It is also recommended that the government set up a fund for NGOs that are set up to help the community fight and educate on cybercrime.

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

The 2019 Unisys Security Index report found that Australians are discerning when it comes to data collection and sharing by organisations, which is a consideration above the technical constraints of sharing information which may be relevant in researching cyber threats and vulnerabilities. For example, two thirds of respondents support the police sharing information with other law enforcement agencies to solve a crime (66% support sharing with agencies in Australia, 65% support sharing with international agencies), only 16% are happy with banks sharing data with other financial service providers to provide a central point of contact for multiple services. More than half (57%) of Australians support doctors sharing an individual's healthcare history with other healthcare providers for a complete view of their health.

A critical constraint is the lack of a common platform to share information and the trust necessary between and within Industry and Government to be successful. In addition, there is a lack of incentives or return for the private sector to participate.

To overcome these constraints, the Australian government could consider setting up a trusted vendor program –in a similar way that the trusted trader program exists with border industries/ importers. After vetting and under strict controls, more sensitive information can then be shared by Government to help industry counter cyber-attacks or develop better capabilities. Transparency with citizens on the potential and limitations for personal information being shared will be a critical success factor.

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

Completely agree. When consumers are unaware of cyber risks, they are likely to purchase / download products that introduces risk. User education is similar to the concept of 'buyer beware' for physical goods and services. The Government can assist here by setting up programs and resources that consumers can access to educate themselves on cyber security and can then use this knowledge to make more informed choices.

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

This will drive the right behaviours as consumers will demand secure products at time of purchase. Businesses found not delivering secure products will likely suffer reputational damage and their market negatively impacted. This is backed by the Unisys Security Index, 2019 which states "15% of consumers stopped dealing with the organisation responsible for losing their data. 12% of consumers publicly exposed the organisation responsible for losing their data via social media. 10% of consumers pursued legal action over personal data loss."

In order to achieve this change in behaviour, user education is key that the Government can assist with. Further, legislation should be introduced to compel businesses to clearly articulate the cyber security features of their products. User education combined with this transparency from businesses will allow consumers to make the right choice and elevate those businesses that are manufacturing cyber secure products.

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

Anti-smoking campaign is a great example. Scale was achieved through media advertising and educational campaigns. Results were easily evaluated with the reduction in the number of smokers – old and new.

A feature of this campaign was the open and transparent (potentially horrific) access to information for citizens in order to support a personal motive for action. Education is the key through mass media and personalisation is the tool to ensure the message gets home.

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

Yes, as well as clearly articulated. This way the consumer is aware and can choose the right products. This is similar in approach to advertising Australian content in food sold in Australia giving consumers the choice.

Legislation should be introduced to compel businesses to clearly articulate the cyber security features of their products. User education combined with this transparency from businesses will allow consumers to make the right choice and elevate those businesses that are manufacturing cyber secure products.

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

A strategy on its own will not achieve results unless it is backed by a clear operational plan. This will need to be underpinned by regulation particularly for critical infrastructure and backed by clear enforcement and penalties. The Government should have the right to remediate vulnerable critical infrastructure networks.

A key focus has to be education of citizens so they can make better and more informed decisions.

Businesses should be incentivised to produce more cyber secure products. This could be achieved via a Trusted Vendor program. Further, legislation should be introduced that protects consumers of cyber goods and services by clearly outlining the responsibilities of manufacturers and associated penalties of non-compliance.

This three pronged approach of education, incentivisation and legislation will operationalise the 2020 Cyber Security Strategy.

Submission by Unisys

Ashwin Pal, Director Cyber Security, Asia Pacific
[redacted]

Ben Silberberg, Public Sector CTO, Enterprise Solutions
[redacted]

Gergana Kiryakova, Industry Director Cyber Security Australia and New Zealand
[redacted]