Submission: Australia's 2020 Cyber Security Strategy

AARNet (Australia's Academic & Research Network)

Final Version 109.0 – 31st October 2019

About AARNet

Australia's Academic and Research Network (AARNet) provides high capacity national and international telecommunications infrastructure and collaboration services for the nation's research and education sector, including universities, health and other research organisations, schools, vocational training providers and cultural institutions. AARNet is a not-for-profit company, owned by 38 Australian Universities and CSIRO, and serves over two million end users who access the network for teaching, learning and research. For more information, visit www.aarnet.edu.au.

Background & Executive Summary

Recent cyber-attacks and a number of high-profile incidents have put the Australian Higher Education and Research (HE&R) sector in the spotlight. AARNet Members and others are increasingly being targeted because of the sensitive data and intellectual property they hold. A number of institutions have indicated that they are seeking additional security operations support to improve their cyber security posture, particularly to augment their staff, skills, and technology, to detect and combat these increasing cyber threats.

We believe that the sector would benefit from greater support from Government in these areas, strengthening the leadership the Commonwealth has shown through the establishment of the University Foreign Interference Taskforce (UFIT). AARNet is uniquely positioned to take a leadership role in helping to safeguard the HE&R sector, and in the implementation of the guidelines to be developed by the UFIT. AARNet operates the network that connects all Australian universities, most publically funded research agencies (PFRAs), a large number of teaching and research hospitals, 1,200 schools, around 40% of TAFEs, most state and federal level cultural and collecting institutions and critical research infrastructure such as optical and radio-telescopes, research facilities and other instruments.

AARNet is responding to this background of increased cyber threat in a number of ways that encompass the entire HE&R sector and, in fact, leverage our place as a part of the Global Research & Education community. We believe that many of these strategic initiatives are critical to improving the security posture of the sector, and would benefit from deeper collaboration with and indeed support from Government.

AARNet is also unique in Australia in that it is connected, both through the telecommunications links it operates, and thorough human relationships, to its National Research and Education (NREN) counterparts globally. The strongest links tend to be with Australia's closest military and intelligence allies, the Five Eyes countries and their NRENs: Internet2 (USA), JISC (UK), CANARIE (Canada) and REANNZ (NZ). By way of example, these four NRENs, with AARNet, are working toward establishing a global threat intelligence sharing capability to support the various cyber security operations projects in their countries.

In addition to the above, AARNet:

1. Is developing a Security Operations Centre (SOC) intended to identify cyber threats affecting its connected institutions in real-time, and to assist those institutions to respond to those threats.
2. Is aiming to establish a cadet program, tightly coupled with its SOC, to help to increase the pool of skilled cyber security workers in Australia. This program may be linked with university or TAFE programs.
3. Is a participant in the Cyber Security Cooperative Research Centre (CSCRC). We believe that much of the new technology needed to address cyber threats will come from universities and collaboration with industry, for example in the application of machine learning to cyber security problems.
4. Is a founding partner in the Australasian Higher Education Cybersecurity Service (AHECS), along with the Council of Australasian University Directors of IT (CAUDIT), AusCERT and REANNZ (Research and Education Advanced Network New Zealand).

Each of these initiatives would benefit from, and be more effective with, further Government support.

AARNet is ready to work with the Commonwealth to help its shareholders and other connected institutions address contemporary cyber threats and safeguard the sensitive personal, research and other information they hold.

Acknowledgements

We would like to acknowledge the support of BDO Australia in the development of this response, in particular Leon Fouche (National Leader, Cyber Security), Charles Sterner, Mitchell Redshaw and Nick Pratley.

AARNet's Response

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

The cyber threat environment as it relates to the Higher Education & Research (HE&R) Sector can be separated into two primary types of concern:

1. High volume, low sophistication cyber-criminal actors, driven chiefly by monetary motivations, and
2. Low volume, high sophistication threats led by state actors with ideological or political motivations.

Whilst financially motivated threats can cause significant damage (for example, ransomware and payment misdirection fraud), these threats can be mitigated to a large extent with basic security awareness, controls and tooling. AARNet's opinion is that the Commonwealth's interests would be best served by focussing upon the second primary type of concern listed above: the highly sophisticated threats led by state actors with ideological motivations, which pose a significant and persistent threat to nationally vital sectors. This applies especially to the NRENs (National Research and Education Networks, such as AARNet) which require an industry wide collaborative approach.

Such collaborations could include intelligence sharing with Government and industry. This may include sector-specific threat intelligence insights or threat actor/campaign tracking, advising the HE&R sector about effective mitigation strategies including Indicators of Compromise (IOCs) for detection and backbone sinkhole capabilities for positive identification of threats, and national cyber security awareness campaigns.

Government should also incentivise and provide more guidance relating to Cyber Threat Intelligence (CTI) sharing, especially to sensitive sectors being targeted by nation states, such as the HE&R sector. Such advice would ideally address three key aspects of CTI:

1. Government guidance and advice must explain the fundamental principles of how any business – large or small – should comprehend CTI. It must develop an operational CTI program for broad use by business. By doing so, Government can empower industry to:
    - Identify and collect relevant CTI from closed and open sources
    - Prioritise and communicate zero-day threats identified domestically and globally
    - Synthesise intelligence in preparation for analysis
    - Prioritise threat intelligence based on a standard, better-practice model
    - Fuse intelligence sources
    - Proactively identify emerging and changing Tools, Tactics and Procedures (TTPs)
    - Disseminate supplementary intelligence reports where necessary to Federal, State and other relevant Government agencies and departments, with ample context and confidence statements;
2. Government guidance should identify its priority intelligence requirements, and its focus-points for private industry, which may include either static or transitory priority intelligence requirements more generally. This approach has multiple benefits, but importantly it postures our nation's private industries to be ready to share important intelligence with Government and other industry participants, whilst also preparing them to receive and action CTI in a meaningful way; and
3. A focus on relationships with sector-specific CTI providers. This is expanded in the answer to Question 3 below.

2. Do you agree with our understanding of who is responsible for managing cyber risks in the economy? *(Protecting government networks, enforcing law, providing advice)*

We observe that despite the responsibility for managing cyber security risks largely falling upon end-users, there is a significant amount of activity in addressing cyber security risks within industry.

Government should provide more guidance to industry and the HE&R sector on acceptable baseline security requirements, particularly where personal and/or sensitive (such as health) information is in question. This guidance should be linked to international standards, similar to the Cyber Resilience Health check (which was based on the NIST (National Institute of Standard and Technology) Cyber Security Framework that the ASX (Australian Stock Exchange) requested from the top 100 listed companies.

The work and guidance that the Australian Signals Directorate (ASD) has provided on the Essential 8 Mitigation Strategies is a positive initiative and has led to improvements in posture within the HE&R sector. However, defining baseline requirements back to an international standard (with which most private sector organisations choose to align) would allow organisations to better benchmark themselves against both their peers and a more widely accepted framework of 'better practice'.

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

Where the opportunity exists, government should encourage sector-wide approaches to addressing cyber risks. This approach will help industries to respond quickly, and in an environment where the availability of cyber security skills is limited. In particular, initiatives where skills, capability, infrastructure and intelligence can be shared across organisations should be encouraged.

Government should seek to form strategic relationships with sector specific/focussed CTI counterparts across private industry, and should capitalise upon these relationships.

There are a wealth of industry Information Sharing and Analysis Centres (ISACs), global NRENs, Computer Emergency Response Teams (CERTs) and private sector SOCs (Cyber Security Operations Centres). Each of these organisations affords opportunities for our national industries to share, grow, protect and collaborate with vital industry and sector verticals. Where Government can open the door to these opportunities, private industry will organically capitalise upon them.

A number of frameworks, such as the Cyber Incident Management Arrangements (CIMA) and systems such as the Malware Information Sharing Platform (MISP) are in place, however these are mostly deployed within Government and larger organisations. Better and closer collaboration with more formal arrangements with vendors and member based organisations such as AusCERT would benefit the nation's industries as a whole; posturing our nationally vital assets to predict threats as they are realised.

In leveraging such an approach, our Government can build resilient national industries which inoculate themselves from potentially disastrous cyber security incidents before they propagate and manifest within our critical institutions.

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

There are three key roles government can play in addressing the most serious threats for Australian businesses and institutions:

1. Funding:
    a. For CTI sharing – this is currently a vendor driven commodity, but with little focus for threats that Australian institutions uniquely face
    b. For expansion of the incident response capability provided by the Australian Cyber Security Centre (ACSC) – where an Australian entity can request government support when dealing with a significant threat actor

c. Establishing a 'Get Well Fund' – remediation for Australian entities that do not have the skills and/or budget to make significant improvements to their cyber defence frameworks and tooling.

2. Baseline advice:
   a. What does 'good' look like, with industry specific recommendations.
   b. Drive a peer group analysis campaign to understand where each institution places on a maturity scale in comparison to their peers, offering tactical guidance on what areas they should focus on based on their current capabilities and deficiencies. This has been done by private industry over recent years with a heavy Australian Pacific (APAC)-Australian focus, and as such, the barriers for Government to partner with private industry to achieve this are low.
3. Legislation:
   a. For CTI sharing, the quality, timeliness and usefulness of CTI will be increased by implementing measures which ensure that organisations are not penalised for sharing CTI in instances where they have been impacted by an incident, or request anonymity. This indemnification support has been demonstrated as a valuable and effective mechanism in recent times within our foreign allies (e.g. active attacks/incidents can be shared without fear of reprisal, either financial or legal; i.e. United States (US) CISA 2015).

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

Government should consider defining minimum baseline security requirements for goods or services, preferably linked to accepted and recognised international standards such as the NIST Cyber Security Framework, refer to our response to Question 2 above.

All goods and services could then be certified or accredited against this and be provided a cyber-rating, similar to the Green Star Energy rating. This concept is already applied within sensitive sectors in the US and Financial Services industry Federal Information Processing Standards (FIPS), or Information Security Registered Assessors Program (IRAP) of the ASD here in Australia for sensitive networks.

Government should consider extending this type of accreditation to consumer goods and include Cyber rating markings on the product to provide consumers with more awareness on the level of security in place for the product.

These ratings could be determined on a quantitative basis, for example taking into account factors such as the number of years of support and hence security updates offered. Not only will this provide an effective mechanism for the consumer to make safer and more informed choices, driving a macro-economic advantage through cost avoidance via cyber-crime and identity theft, it will also collectively uplift the general awareness of cyber security across the nation and within business and homes.

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

There are several ways in which government and industry can work together to increase overall cyber security and digital offerings to improve security, quality and effectiveness:

4. A national rating system indicating cyber security features and maturity inherent to products, services, and overall supply chains, in the energy star style, will in turn build confidence, drive improvements and raise awareness across both the public sector and private industries
5. Increased participation from within industry sectors, particularly those that produce the intellectual property which fuels our nation's development and competitive edge, such as the HE&R sector
6. Building "Centres of CTI Excellence"
7. Incorporating case studies which examine what went well, what went wrong, and what were the benefits of the actions undertaken into public reports
8. Establishing "Industry Specific Task-Forces" which will have the intention of fostering closer public-private cyber security collaboration.
9. Educational, awareness and cultural change reinforcements, similar to the old campaigns of the need to wear seat belts and the health risks of smoking.

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

Three specific market incentives Government should consider include:

1. Funding for HE&R Sector-wide initiatives including the AARNet SOC and the Australian Higher Education Cyber Security (AHECS) programme. Cyber security services provided to the HE&R sector need to be subsidised by the Government so there are no barriers to entry in obtaining these services
2. Incentives for universities to invest in cyber security programs to meet the Department of Education and ASD Task Force guidelines. These incentives would be aligned to the program of work to be developed by the University Foreign Interference Task Force, including the implementation of standards, and to uplift infrastructure
3. Incentives for Universities and industry to hire employees who complete appropriately current and modern training in the field of cyber security.

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

See response in Question 8.

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

There are several ways in which Australian governments can build a market of quality cyber professionals:

1. Funding for educational programs – K-12, University, and post-grad degrees
2. Funding Australia's HE&R industry to mature its cyber capability to both protect itself and educate the next generation of cyber risk management practitioners
3. Funding for intern programs for public-private sector (Ireland-Israel model)
4. Review US models – Palo Alto Girl Scouts (badges)
5. Support industry collaboration and training exercises, for example cyber range and "Boss of the SOC".

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

In relation to our response to Question 1, high-volume, low-sophistication attacks are, at a technical level, dealt with effectively by current vendor technologies.

As vendor technologies increase in sophistication, with respect to this threat, our opinion is that government's support would be best placed in cyber security awareness training.

Since these types of threats commonly exploit human error, awareness training can serve as a targeted, and cost-effective method to:

- Collectively raise security awareness
- Posture the people powering our industries to proactively defend them
- Reduce the national cost of cyber incidents, and
- Simultaneously support the ongoing development of existing vendor capabilities such as email security.

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

Government should aim to disrupt the economics that incentivise threat actors by fostering good security hygiene:

- A vast majority of adversaries leverage low sophisticated attack methods, which can be easily overcome by basic security controls such as multi-factor authentication, endpoint protection, and data encryption at rest. Similarly, most organisations can effectively respond to and overcome commodity threats through proper planning and preparation via cyber security incident response plans and exercises
- Adversaries must invest time, money and motivation, and the more robust the target environment, the more likely the adversary is to move on. Though this may not be enough to overcome highly sophisticated adversaries, it nevertheless reduces the impact cost of an attack whilst slowing the adversary's progress. This can provide

invaluable time to coordinate an effective response against even the most motivated threat actors.

Government should encourage industry to perform their defence capability holistically, including prevention, detection and the ability to respond. This is especially helpful as those with lower maturity can benefit from those with higher maturity.

- Prevention is an investment in security controls. Threat sharing of known adversaries and their attack methods allows others to inoculate themselves through security device rulesets and sink-holing of IP addresses for example, forcing the adversary to continually invest time, money, and motivation
- Detection is the sharing of Security Information Event Management (SIEM) correlation rules, IOCs, investigation playbooks and other detection methods to aid others in finding adversaries
- Share mitigation strategies and techniques to allow the industry to learn and adapt from each other with playbooks, workflow orchestration and other effective tools.

When this concept is coupled with the aforementioned investment in baseline security controls, which includes a focus on CTI sharing, industries help themselves and each other to raise maturity – recognising threats, areas of risk, learning lessons – and then share these with each other in constructive ways.

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

Principal ways in which governments and private entities can help remediate cyber risks on private networks include developing trusted partnerships, threat sharing and developing industry and sector-wide SOCs:

1. Trusted partnerships – Developing ways where resourcing can be a shared responsibility to ensure a cross section of skills are available to provide appropriate and timely responses to an incident or potential incident
2. Threat sharing – Develop mechanisms where IOCs are most appropriately matched to the relevant system and sector's vulnerabilities such as banking and telecommunications, and if there is more sensitive compartmented intelligence, ensure this is still shareable with detection and remediation, following appropriately matched compartmented paths to ensure protection of threat sharing pipeline
3. Industry and sector wide SOCs – Develop a collective type scenario where there are incentives to develop and maintain SOC's and associated services for specific industries. There are generally many barriers to entry to develop these types of services where competition outweighs the driver to collaborate. Security needs to be treated as a team exercise for industries and this will be much easier to achieve with government support.

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

The private networks that Government should consider to be critical systems that need the strongest cyber defences are those networks covering education and research, records of national significance, and personal records:

1. Education and Research networks – These networks are used by more than two million Australians and contain significant amounts of PII (Personally Identifiable Information) and sensitive research information
    i. Personal records (e.g. student records) – Recent media reporting has highlighted the ongoing value and active targeting of this type of data for many reasons across various actor groups
    ii. Intellectual property – The Australian Education Sector produces vast amounts of world leading research which is being actively targeted in fields like medical, technology, government and defence.
2. Records of national significance – AARNet provides communications for many organisations where records of significance are held on both public and private networks. These can include Government archives through to supercomputer research networks across the country
3. Operational Technology (OT) and Industrial Control Systems (ICS) associated with institutions of national significance/criticality. From AARNet's perspective our customers in this space include universities, research facilities (both Government and private), Kindergarten to Year 12 schools, galleries, libraries, archives and museums.

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

Funding models that government should explore for community protection would include support for targeted, sector-specific initiatives including co-investment in the areas of:

1. Education and awareness training
2. A 'Get Well Fund' for assisting with implementing the Essential 8 Mitigation Strategies or other corresponding baseline
3. Threat sharing
4. Industry-specific, collaborative security initiatives and services for industries of the type identified in our answer to Question 19. AARNet's sector-wide SOC project is one such example.

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

Readily identifiable constraints to information sharing between the public and private sectors in relation to cyber threats and vulnerabilities include:

1. Risk appetite – There is a current challenge in declassifying IOCs to allow them to be acted upon under controlled scenarios. Ideally there would be a mechanism where

more sensitive IOCs can be provided to operators of critical infrastructure, such as AARNet, to ensure proactive detection and remediation of advanced threats

2. Resourcing – Due to budget and market forces, the expertise needed for collaboration is not accessible to all organisations to best leverage threat intelligence appropriately, especially in the Server Message Block (SMB) case
3. Indemnification framework – Ensuring there are sufficient protections for responsible sharing of information through moral obligation arising from activities outside of the white hat roles
4. Distrust of government (public) – There appears to be a level of distrust of Government portrayed through some media channels which can make broader collaboration more difficult. There is a good engagement with larger corporate entities and critical infrastructure but sometimes this does not extend far enough or in a timely fashion
5. Understanding of incentives and the benefits of sharing – Articulation of the value proposition for organisations in actually sharing information, when there may be no immediate payback. Best analogy is immunisation and herd immunity, but this needs to be a cultural development where in many cases it costs time and intrinsically money to perform this function and many organisations are not resourced appropriately to undertake sharing.

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

Government is doing great work through the StaySmart Online partner program, however it should consider extending the scope of this initiative to the wider public and provide more media publicity and awareness of the online cyber threats to consumers (similar to the "Stranger Danger" initiatives in place for child safety, or "Don't Drink and Drive" campaigns).

From a corporate and business perspective, Government should conduct, facilitate and encourage cyber-readiness exercises at both sector vertical and wider industry levels in order to test and rehearse organisation and business preparedness to respond to and recover from relevant, likely cyber incidents or attacks.

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

Yes. This is already happening with success, for example, with Microsoft's Azure and Amazon's AWS security offerings. These are being driven by customer demand, and their implementation is increasing the competitiveness of these platforms, for example through IRAP certification. Caution must be used to avoid providing a false sense of security, however. The built-in security features should align to a common set of security principles, and clarity will be needed to understand what security control gaps remain.

[END]