Queensland University of Technology

Submission in response to

Australia's 2020 Cyber Security Strategy – A call for views

Queensland University of Technology (QUT) is pleased to provide a submission to the Department of Home Affairs discussion paper *Australia's 2020 Cyber Security Strategy – A call for views.*

Australia's 2016 Cyber Security Strategy set out the Australian Government's plan to strengthen cyber resilience and security. Under this strategy the Australian Signals Directorate (ASD) became the single point of cyber expertise for the Australian Government, and Joint Cyber Security Centres (JCSC) have been opened across the country to work more closely with industry. This discussion paper seeks to explore how Australia can build on this foundation and position itself to meet cyber threats now and in the future.

QUT's submission draws together the collective thoughts from QUT's Information Security team who provide cyber incident response, risk management services, and security awareness programs across the institution's functions of Learning and Teaching, Research, and Administration. Should further information or clarification be required for this submission, QUT welcomes the opportunity to expand in further detail.

Discussion Questions

1. **What is your view of the cyber threat environment?**

   The cyber threat landscape continues to evolve and is evident through sophisticated threats resulting in more significant impacts. The main attack motives still remain focussed on cybercrime for financial gain, data and intellectual property theft, and disruption activities such as ransomware and Distributed Denial of Service.

   From a Higher Education perspective, 'Nation State' attacks are of significant concern. Notably, in 2019 there were two publicly disclosed cyber intrusions of the Australian National University (ANU) that are believed to have involved sophisticated nation-state actors.

   What threats should Government be focusing on?

   The areas of cybercrime and Nation State attacks are of the most concern and warrant continued Government focus and progress of activities. As echoed in the 2020 Strategy, both of these types of attacks have potential material impacts on both individuals and the Australian economy, as stolen intellectual property reduces competitive advantage. These types of threats cannot be completely addressed by individual organisations.

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

   The responsibility for managing cyber risks in the economy rests with Governments both State and Federal, and it is expected that Governments would coordinate to develop the frameworks and risk treatment programs. Additionally, QUT recognises that at an organisational level there is also an accountability to our own cyber security and that at an individual and local level we must do all that we can to assist in the security of our cyberspace.

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

   The overall ownership of risks relating to cyber security remains with the Australian Government, but the responsibility to develop and support a cyber-aware community is borne equally by Government, businesses and individuals.

   What changes should we consider?

   There would be significant benefit in making education campaigns more continuous. To date, there has been a reliance on 'special events' like Privacy Week or Stay Smart On-line week, where more continuous campaign and education roll-outs would be more effective in raising awareness and changing attitudes and culture.

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

   There needs to be a well-defined set of protocols to facilitate the exchange of highly sensitive threat data when serious Nation State attacks are in progress. It is important these exchanges are handled properly to avoid impacting ongoing remediation activities. In these situations, government should have powers to compel organisations to commence remediation.

   Nation State actors often use new attack methods that are not easily identified by individual organisations. Often these methods have been previously identified by the Australian Government Intelligence Agencies, but not necessarily publicly released until investigations are completed. This means that in some circumstances the Australian Government agencies will be aware of compromises of national significance, but are unable to share information securely with other industry partners that have not yet been targeted.

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

   To maintain trust levels the Australian Government needs to seek and take the advice of technical and legal subject matter experts, so internet regulatory decisions are beneficial to the whole community, including consumers, industry and law enforcement agencies. The creation of a balanced framework that includes regulation, policy, education, awareness and support for industry is an important foundation. Commitment to the implementation of the framework will also go a long way to ensuring that the community at large does not either feel imposed upon or that 'someone else' will deal with cyber security.

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

   In some international jurisdictions, laws are already in place to strengthen customer protections by legislating common-sense approaches to default configurations. The State of California in the United States recently passed legislation to require manufacturers of internet-connected devices to incorporate in their products 'reasonable security measures to protect them from unauthorized access, use, destruction, disclosure, or modification by hackers'. Additionally, the European Union (EU) has developed some certification levels that applies to security products, so that consumers can understand the specific security features of particular products. The Australian Government should endorse and emulate this approach, looking to expand it into the Australian goods and services sector. As Higher Education moves towards a more 'Bring Your Own Device' approach this will be critical in ensuring that institutions have a base level of protection from cyber-attacks.

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

   Both Government and industry have to continue to educate users at all levels of the community including – small- and medium-sized businesses – about cyber safety. Continuous campaigns of focussed education are a key element to making the Australian public more cyber-aware.

   Options to improve first lines of our defence at our cyber borders should be explored. In light of the strong argument for national benefit accruing from a united defensive effort, this should include providing programs to assist telecommunication carriers and Internet Service Providers (ISPs) to invest in these defences with a minimum flow on-cost to the end consumer.

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

   The Australian Government needs to maintain levels of trust with the community and not adopt measures that negatively impact the reputation of cyber security in Australia. Additionally, an approach to endorse and facilitate continuous improvement and best practice in the development of cyber security would be highly beneficial. Support for Centres of Excellence in this arena within Higher Education would be a particularly efficient way to promote the rapid development of work in this area required to keep up with the speed of development characteristic of motivated hostile actors. In the absence of a cohesive and recognised industry body, Government should consider taking a role in defining cyber certifications. Examples from other industries and jurisdictions could be used as a starting point.

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

   None at this time. The private sector is simply not mature enough for us to transfer essential national defence capability away from public management.

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

    The current regulatory environment is appropriate. There are a number of international standards that organisations can choose to comply with that build in a good set of security controls. There is no case for developing and mandating any new security standards: indeed, by diverting effort onto an additional compliance regime that adds no discernible value, it would only increase risk.

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

    Due to the reduced Australian Government funding contributions to Higher Education there has been a reduced spend on advanced technology solutions and therefore cyber security. The Australian Government could consider allocating cyber-specific funding streams or other financial and taxation incentives for cyber investments. Research & Development (R&D) activities should be encouraged to operate and come to market in reputable environments that facilitate modern and innovative outcomes. A premium rate for cyber security R&D within the R&D tax incentive scheme would be one mechanism.

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

    As mentioned above at 6, leading international jurisdictions such as California and the EU have already enacted laws to this effect. The Australian Government should deploy this approach for the Australian context.

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

    The Australian Government could establish a 'Register of Compliance' where industry organisations could voluntarily provide evidence of cyber security certifications. This would enable an individual or organisation to validate that a proposed supplier has some cyber-security controls or frameworks in place.

    As a significant procurer of technology, perhaps even acting as a lead agency for federated public sector deals, the Government could increase cyber security requirements for its own procurement. This could include standard clauses in contracts, the requirement to reach a certain standard for targeted technology products and services, and offering consulting advice to agencies and other entities utilising these agreements.

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

    Identify and understand the aptitude required for being a cyber-security professional, seek out these talents and offer flexible programs that encourage development in the profession. Additionally, to keep people in the industry, flexible work and transition to retirement options may encourage more experience practitioners to remain in the workforce to mentor and coach new entrants to the industry. More prominence of specific standards and qualifications supported and endorsed by the Australian Government would aid in building cyber security capability within the Australian employment market.

    Whilst developing cyber security professionals is important, recognising that varying degrees of skills and awareness are required in other professions is equally important.

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

    Cyber Insurance is not seen as a 'value for money' investment, because there is too much ambiguity and complexity in policies. As a result the actual coverage provided is not well understood. Also, many insurance products are provided by international insurers and are not tailored to the Australian marketplace.

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

    While a technical implementation that consists of utilising mature threat intelligence capabilities to identify and block known malicious activity at the ISP is possible, this type of solution could have the effect of adding unreasonable cost to consumers.

    Strategies to block malicious traffic at the national level have been proposed in different forms on previous occasions and have only contributed to distrust of the Australian Government. Working in partnership with ISPs and telecommunication carriers to increase their capacity and capability in cyber security would be more likely to be effective.

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

    Reducing incentives including the profitability of malicious activity could be achieved by improving cross jurisdiction support for law enforcement, aligning a contemporary legal framework with the digital world, adopting global frameworks, improving public education on the issues, and adhering to forward risk-minimising policies such as not paying ransom demands. Mitigating risks in other channels of compromise such as telephony and SMS must also be pursued, and criminality in inter-dependent processes such as money laundering should be actively dealt with.

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

    Current frameworks do exist in industry to meet this need. Adopting a national standard and reducing the barriers to entry in threat intelligence sharing for the whole business community may help. Improving the transparency of business adoption of standards such as ISO27000 can also act as an incentive towards adopting good practice.

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

    The Australian Government already knows the critical systems it needs to defend, and has developed additional security compliance standards for organisations that provide essential services to the community including power, water, gas, communications and ports. There are provisions within the existing *Critical Infrastructure Protection Bill 2018* that could be enacted and enforced.

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

    Continued funding to JCSC, funding of broader community awareness campaigns and small business education. Tax incentives could be considered for organisations that are actively investing in improving cyber security capability.

    Funding for JCSC could be modified and extended to create state-based centres of excellence to facilitate work integrated learning opportunities for students and encourage bidirectional exchange of skilled individuals between industry and academia.

    Awareness campaigns need to be stratified, sustained and omni-channel. The current event-driven approach is ineffective. Lessons could be drawn from exemplars in other subject areas like health and safety, consumer protection and road behaviour.

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

    Constraints include the potential disclosure of corporate vulnerability information to competitors that could then be exploited for market advantage. Additionally, there could be fear of reprisal or litigation resulting from the public disclosure of untreated vulnerabilities. There are still class action cases pending relating to the Equifax breach in 2017.

    A lack of trust may also derive from the belief that Government does not share the same rules of responsible disclosure or attribution.

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

    QUT strongly agrees that there is a lack of cyber awareness driving poor consumer choices. Low costs in conjunction with a poor understanding or lack of concern of the true consequences to both the individual and the broader community often drives poor user behaviour. As mentioned previously a complete revamp of cyber awareness with requisite investment is required to materially shift community awareness and attitude through a stratified, sustained and omni-channel approach.

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

    The introduction of standards or certifications for cyber security products will help to educate consumers about minimum expectations of cyber security incorporated in products. This will enable consumers to demand more secure products which will in turn drive the supply lifecycle.

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

    None at this time in this domain. For an exemplar that warrants emulation the Australian Government should look to its own highly successful antismoking campaigns, which were accompanied by timely and rigorously enforced regulatory reform.

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

    Cyber Security features should be promoted on all products and services. Ideally a consumer rating would be used that reflects a risk assessment measuring both the product and the company's existing frameworks. A similar approach to the EU certification levels to Cyber Security products should be considered.

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

    The strategy must be accompanied by a funded action and implementation plan with accountable owners and timeframes. If the aim of the present exercise is to achieve incremental improvement then a few changes to the existing approaches and programs would do. But if the aim is to significantly increase awareness, behaviour, capacity and capability – as it should be, if we want to stay ahead of likely threats – then the strategy needs to reflect that fundamental shift. The latter would certainly present a better outcome for the nation, for the sector and for the public.

    Whichever way it falls, the strategy needs to be backed by funding and an action plan. Any other approach would suggest lip service.