Huntsman®
Defence-Grade Cyber Security

Australia's 2020 Cyber Security Strategy – A Call for Views

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

The cyber threat environment is busy, complex and ever-changing. Organisations can easily become disorientated about how to manage their cyber defences. Rather than focus on any one specific threat, Government's role should be to establish methodologies and guidance that support the achievement of a foundation level of cyber resilience for all organisations; the established ACSC Essential 8 security framework is ideally suited. Government can assist organisations by providing a clear, progressive and manageable template for the establishment, measurement and improvement of their cyber resilience management process.

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

There is no doubt that Government should take a leading role in the management of cyber risks in the economy, however, organisations themselves should be held responsibility. The Government should champion and encourage improved cyber resilience so the economy becomes less vulnerable to the constantly changing risk landscape.

A strategic plan supported by frameworks, methodologies and on-going leadership is required to achieve improved resilience ambitions.

The establishment of ACSC, AustCyber State Nodes and the Notifiable Data Breach scheme go a long way to providing infrastructure to support communication with Australian business. A coordinated effort across these channels is now required to support implementation of an operational plan that will assist the ongoing performance improvement cyber resilience across the economy.

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

The next logical step in managing Australia's cyber risk would be to provide a practical route for 'how' this can be achieved. Specifically, the July 2019 ISM document provides, in great detail (183 pages) 'security outcomes' to be achieved by organisations; in our experience, security practitioners need something more than a performance specification. For example, within the 'selecting security controls section' it presumptuously states:

Using a risk assessment, select security controls for the system and tailor them to achieve an acceptable residual risk

To assist a greater number of security practitioners, best practice recommendations should be provided in terms of what security controls should be selected. The Australian Government's own

Essential 8 security controls, and better guidance as to how they can be implemented and managed on an ongoing basis would be invaluable for many organisations. This would empower Government departments and business to follow tried and tested templates to support greater cyber resilience, using a framework that have been found by ASD to mitigate 85% of targeted cyber-attacks and currently forms the basis of the ANAO IT security audit programme.

See, for example, APRA's latest corporate plan for the Financial Services sector, most importantly it defines the strategic focus area for the improvement of cyber resilience on Page 16, then proceeds to detail strategy execution, measurement and accountability in chapters 4 and 5.

Question 4 – What role should Government play in addressing the most serious threats to institutions and business located in Australia?

Government should first lead by example, as was originally proposed, by implementing a cyber resilience improvement plan with the Essential 8 security controls as its framework across its own departments. Then, as the ANAO audits have confirmed, the success of that implementation and any improved cyber resilience can be measured as part of an ongoing performance improvement programme. Critical Infrastructure businesses (including Financial Services and Banking), if they are truly considered to be critical to the ongoing stability and operation of the economy, should also be directed to achieve a pre-determined level of cyber resilience against the model. If, as quoted by ASD, up to 85% of attacks can be reduced through the effective implementation of E8 controls, simple arithmetic would suggest that any "under-utilised" resources released as a result of improved E8 controls could be redirected to the remaining 15% of attacks with significantly greater (up to 6 times) effectiveness. . A level of continuous visibility will enable Government to prioritise its support and intervene when the risk environment demands it or the levels of cyber control effectiveness fall.

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

Maintaining trust in the Government's cyber security capabilities can be achieved through leadership i.e. leading by example. We have an Ambassador for Cyber Security, promoting the importance of a secure, lawful and socially responsible Internet across the region; the next step is to create a practical plan to implement, monitor and support those initiatives, starting in Australia, by demonstrating actual on-going improvements in cyber resilience and confidence in on-line dealings with government departments.

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

A system that encourages and ultimately obliges (lead time to adoption) supplier or partner organisations to publish a Cyber Resilience Trust Index (think 5-Star rating) would provide customers a tangible measure of confidence in the trustworthiness of a suppliers' products and IT systems. The index would enable organisations to identify and compare suppliers and, indeed their goods or services, in terms of how secure, reliable and fit for purpose they truly are.

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

A requirement for suppliers of goods and services to establish a Cyber Resilience Trust Index and publish their measure of compliance against an credible and easily understood cyber security framework is an important consideration. The E8 Risk mitigation strategies are one such framework. In an increasingly connected economy, the concept of Zero Trust resonates beyond the enterprise and 3rd party suppliers. A cyber resilience score measures the cyber trustworthiness of a supplier; the higher the cyber posture score the greater the confidence gained by consumers. Through competitive market forces and a public campaign for greater protection for consumers, cyber resilience will become a business asset for suppliers.

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

The results of the ANAO cyber security audit programme over the last few years confirms that security, quality and effectiveness of cyber security can't be adequately delivered without an active management effort. Subjective questionnaires and self-management is not working and any measurement or assessment of trending and performance improvement requires verification and audit.

For effective management Government, or its delegate, must undertake regular and ongoing performance measurement of security posture in each department. There are two things the small number of costly ANAO cyber resilience audits have demonstrated: (i) there is a need for a more streamlined audit and management methodology and; (ii) even the largest government departments with all their resources, technologies and processes are struggling to achieve even the mandated 'Top 4' security controls.

Government needs to digitally transform the audit and ongoing management process to deliver an easier path to cyber resilience. By automating performance measurement against the Essential 8 security controls, the Government could industrialise the cyber resilience management process and gain visibility of the current and on-going state of resilience levels over time, against a common standard framework. Leagues tables and balanced scorecard techniques for comparative management and management by exception are two real management possibilities.

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

By introducing digital transformation into cyber security auditing, Government monitoring and reporting endeavours could be replicated and devolved to an administrative organisation or, indeed, the private sector. Government supervises the governance of the financial services and banking sector with laws, sector regulators, directives, structure and enforcement. Cyber Security should follow suit.

Australian Federal government organisations are mandated to comply with the 'Top 4', a subset of the 'Essential 8 Security Controls'. Additionally, they are obliged to comply with the Australian Information Security Manual (ISM), so they must regularly assess security controls to make sure they are implemented correctly and operating as intended. Parts of the framework are already in place; it's the ease of establishment of the measurement processes, the reporting mechanics and the management regime that requires implementation. After all, in a digitally transformed world much of the activities around reporting, performance assessment and remediation management will be administrative rather than technical in nature.

Much of this supervisory work could easily be devolved to the private sector or to individual industry regulators who could then undertake performance management within their respective industries. The digital transformation of E8 audit to a continuous process is the new RegTech.

By using the Essential 8 security controls as a baseline across all Government departments regulators or even the private sector could use transformational RegTech to clearly and objectively benchmark and monitor resilience performance managed.

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

There are two noteworthy issues that emerge from the Federal Government regulatory cyber security environment: (i) Operating within the environment is not yet a systematic and documented process that can be supported by smart technology; rather it still relies on high level security specialists for its operation and management; (ii) It is not yet sufficiently well-defined at the security control level. A systematic audit process against a standardised cyber security framework would simplify the regulatory environment and reduce the reliance on scarce cyber experts, for its operation.

Government needs digital transformation of the audit process to enable a strategy that is comprehensive yet effective at scale. It needs one that provides timely information to enable ongoing monitoring and feedback for continuous improvement of cyber resilience.

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

The regulatory requirements do not need to change, they simply need to be industrialised onto a comprehensible system for ease of automated digital measurement and effective management. This is as much a scale as a performance problem and technology can provide the benefit of streamlined repeatable processes that can deliver continuous and reliable compliance and risk management reporting for improved cyber resilience.

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

Establish a set of requirements and performance standards, that can be verifiably measured for the management of cyber resilience. A trust index or measure of compliance to built-in cyber security requirements will attest to the improved security performance of digital goods and services.

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

We know in the US that >60% of cyber-attacks on corporations are from 3rd party sources (HBR July 2018); and there is little to suggest that the situation is that different in the Australian public sector. Hence the introduction of 3rd party cyber security posture auditing of supply chains against the Essential 8 security controls will greatly assist the cyber resilience of both the buy and sell sides of any supply chain relationship. This continuous E8 monitoring could be done using an automated measurement tools such as: the Essential 8 Auditor, for smaller organisations, or; the Essential 8 Scorecard for larger firms to quickly instil improved trust into supply chain relationships.

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

The creation of a market of high-quality cyber security professionals is a never-ending and lengthy endeavour in an environment where there is more and more data to process and more threats to defend against. Given the growing delta between resource supply and demand, any solution must include a combination of training more skilled professionals, streamlining security process workflows and automating technology to support security outcomes that reduce the need for human intervention while ensuring on-going expert oversight, as necessary. By automating workflows and routine tasks and improving the performance of security technologies organisations can become more systematic, reliable and efficient in their security operations which will in turn deliver improved cyber resilience.

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

As it currently stands there is no one, practical, industry agnostic model used to objectively and more accurately measure an organisation's unique risk. There is, however, a definite trend by underwriters recently to increase the levels of risk assessment for cyber security insurance. By introducing a recognised methodology and framework, such as benchmarking performance against the Essential 8 security controls, the cyber insurance market would be able to measure improvements in overall cyber resilience and residual risk for an organisation and hence ensure cyber insurance becomes a legitimate and efficiently priced risk management tool across the economy.

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

We need to better understand the actual vulnerabilities being exploited in these types of low sophistication attack. We need to understand the underlying disease as distinct from the symptoms. Whether it is attacks from nation states or elsewhere, many of these attacks are actually taking advantage of poor underlying cyber hygiene across the economy. When it comes to attack numbers and disruption to the economy think about the 80:20 rule or maybe even the 99:01 rule. In

September 2019 in 'Rethinking the Security and Risk Strategy', Gartner noted that even by the end 2020, 99% of successful cyber-attacks will continue to be the result of already known vulnerabilities.

Organisations can improve their basic level of cyber hygiene and as a result their resilience through implementation of Australian Government's Essential 8 security controls. ASD advise that effective implementation of these controls can mitigate up to 85% of cyber-attacks; Automated tools such as Huntsman Security's Essential 8 Scorecard can support the ongoing measurement of the Essential 8 security controls effectiveness to enable reduced risk exposure to low sophisticated attacks.

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

As per question 16, while the government cannot reasonably limit attacks it can certainly improve Australia's preparedness for them. If we want to truly protect our economy from cyber threats then digital transformation of cyber security management process is a must. Again, a standardised framework for measurement and management, more specific guidance and automated tools could support raising the basic level of cyber resilience through the establishment of a baseline of cyber security competence.

Question 18 – How can governments and private entities better proactively identify and remediate cyber risk on essential private networks?

By undertaking continuous monitoring, timely reporting and regular auditing of their security control effectiveness.

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

It all starts with risk assessment and the establishment of which networks and IT assets support the transactional activities with, or storage of, valuable or sensitive information. Yesterday sensitive government information, this morning superannuation customers and tomorrow, maybe, medical information; and harvesting of any type of valuable information is the recognised business of nation states, not just criminals.

In addition to all Government departments and agencies, the priority private networks should include organisations within the health records and critical infrastructure sectors i.e. utilities, transport, telecommunications and financial services & banking. It would seem reasonable that, if Critical infrastructure organisations can be identified as critical because of their importance to the economy, they should be required to maintain higher levels of cyber resilience. GDPR legislation is starting to show its teeth in EUR and similarly in the US, organisations, large public and private organisations that process or store personal information are, at the risk of penalty as they become increasingly obliged to list assets that need to be actively protected and secured.

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

The introduction of an incentive / reward scheme for organisations to actively measure cyber resilience against the Essential 8 security controls is important step, particularly for organisations which might not be risk averse or may even be ambivalent about additional cyber security investment. Behavioural change often requires encouragement; the risk of failing cyber security compliance levels may be sufficient encouragement for some to improve their resilience; but not for all.

We spoke earlier of enforcement being a critical part of behavioural change but carrots could include: (i) promoting 5 Star security businesses; (ii) requiring that all government supply chain participants, meet particular cyber resilience levels without exception; and even (iii) organisations with verifiable maturity level 3 Essential 8 compliance levels could be granted investment tax concessions for achieving and maintaining that level of cyber resilience. This could apply across the economy or only for small and mid-size organisations that require assistance to meet improved levels of cyber resilience.

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

Australia now has Notifiable Data Breach requirements that supports information sharing and reporting between organisations and government. The Basel Committee on Banking Supervision noted in their Cyber Resilience: Range of Practices report in Dec 2018, that while some jurisdictions had information sharing between some parties Regulators and Banks generally the sharing of all types of information freely between all parties is the exception rather than the rule. For example, in order to support better multilateral communication between parties Government could initiate a Weekly Threat Report, like the one established by the NCSC, in the UK to better communicated observed threats out to business.

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

Undoubtedly a lack of cyber awareness drives poor consumer choices, and not knowing a basis upon which to start in not uncommon. Regardless of an individual's level of cyber security maturity, an awareness of the cyber trustworthiness of the supplier and how a product or service aligns with a particular security frameworks will level the cyber awareness playing field between buyer and seller. By focusing on implementing, managing and publicising the effectiveness of good cyber hygiene, using the Government's Essential 8 controls for example, organisations can raise their knowledge and at the same time educate their consumers as to the benefits of improved cyber awareness and greater cyber resilience in their on-line activities.

A public awareness program from the Government to improve cyber resilience with information available to both business and consumers could also certainly improve cyber awareness and the demand, at all levels of the economy, for cyber resilience.

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

By providing consumers with a measure of any given product's cyber quality is of assistance in improving their purchase decision making. By introducing an Australian scheme where creators of cyber security products can declare and verify their level of cyber resilience i.e. using scoring metrics and an acknowledged 3rd party security framework, products or services can be confirmed as being fit for purpose as well as from a vendor's perspective create sales differentiator, raise awareness and support greater market driven focus.

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

There have been a number of successful public health campaigns in Australia over recent years, each one ultimately driven by people's concern about their own welfare and the high public health costs of smoking, skin cancer and even AIDS. A similar successful cyber awareness campaign would improve people's cyber understanding, encourage their willingness towards behavioural change and ultimately save the economy significant amounts of money. Comprehensive awareness campaigns have been shown to work in Australia that were ultimately measured as making a difference were:

- Slip! Slap! Slop! - to reduce the incidence of skin cancer in young adults
- Smoking – to reduce the rates of people smoking, fewer people dying
- AIDS – to contain the spread of HIV

In 2018, the Public Health Association of Australia said of successful campaigns "Continued funding, promotion, enforcement and improvement of policies remains essential".

There is no doubt that prevention is always better than cure. Cyber resilience, while not a life-threatening problem, will cost the economy increasing $billions. In order to, mitigate risks organisations must first understand where to start. By creating a 'how to achieve compliance to the Essential 8 security controls' capability for smaller organisations, and helping consumers to understand why they might benefit from "cyber safe" products will assist in creating a virtuous cycle of better cyber behaviour.

Already in the US organisations are talking about Trust Indices, organisations are offering security ratings just like credit ratings and stakeholders across the economy are starting to listen. Customers are starting to question organisations who have signs of poor cyber history; finding another provider of that same product or service is easy. Good verifiable security ratings or cyber resilience metrics will ultimately be a USP for all stakeholders across the supply chain.

Question 25 – Would you like to see cyber security features highlighted in products and services?

As per the response to question 23 cyber resilience is an asset to any business. For example, by introducing a Trust Index into the supply chain transactions will enable buyers and sellers to make

informed choices as to the trustworthiness of an organisation and the associated level of residual risk they are exposed to.

Question 26 – Is there anything else that Government should consider in developing Australia's 2020 cyber security strategy?

To ensure an economy of cyber-savvy participants, government needs to provide frameworks, directives and proven operational model templates for broad adoption. Incentives and/or enforcement strategies to encourage behavioural change are also an important part of achieving the improved cyber resilience that is so fundamental to protecting a transformed Australian digital economy.

Whilst the above aspects are fundamental to success, it will only be through introduction of industrialised operational processes of implementing, automated monitoring and timely reporting and auditing cyber security controls that Government and business can continuously improve cyber resilience.

About Huntsman Security

A private company founded in Sydney, Huntsman Security has expanded to Canberra and London, with operations in Tokyo and the Philippines. The company serves customers in the Defence, Intelligence, Government and Critical Infrastructure sectors as well as providing automated continuous IT security risk audit and reporting technology to the wider market.

https://www.huntsmansecurity.com/company/