THE FUTURE OF AUSTRALIAN CYBER SECURITY

A Response to "Australia's 2020 Cyber Security Strategy: A call for views"

Department of Home Affairs

01 November 2019
Matthew Graham
General Manager Strategy
Ph: [redacted]
[redacted]

OUR UNDERSTANDING

As the overarching body responsible for Australia's cyber security strategy, the Department of Home Affairs (the Department) is seeking views from the Australian community on the future direction of the 2020 Strategy, as outlined in the "Australia's 2020 Cyber Security Strategy: A call for views" paper (2020 Paper). As a well-established consulting firm for government, Defence and national security, Noetic Group (Noetic) welcomes the opportunity to provide a contribution based on our experience to the Department on the future cyber security strategy.

The introduction of the 2016 Strategy was an excellent foundation for Australia's approach to cyber security, providing essential services such as the establishment of the Australian Cyber Security Centre (ACSC). However, with increasing reliance on technology and the expansion of online connectedness, the 2020 Strategy must continue to evolve with the rapid pace of change in the cyber domain. This continual shift in the cyber domain has caused Australians to be become increasingly susceptible to cybercrime, such as that recently demonstrated by the attacks on ANU, the Australian Parliamentary network, Victorian hospitals and the proliferation of EMOTET. These highly sophisticated attacks are often socially engineered to exploit human behaviours, with one click being the difference between a successful or unsuccessful cyberattack.

As a management consulting firm, Noetic does not work extensively in the IT and technical capability fields. We do, however, understand the business of government and industry and have significant experience in helping such organisations deal with complex enterprise risks and the identification and implementation of critical controls that prevent those risks from being realised. We also have a strong appreciation for the human factors that contribute to organisational failure and those that underpin successful implementation of initiatives and meaningful monitoring, evaluation and learning (MEL) strategies. Whilst these are non-technical approaches to cyber security preparedness, we believe the recommendations in this submission will provide useful insight into the formation of the 2020 Cyber Security Strategy. This response answers select questions proposed in the 2020 Paper, and discusses other key areas Noetic believes are important under the following topic areas:

1. Awareness Vs Action
2. Understanding What's Important: Looking Through an Enterprise Risk Lens
3. How Everything Fits Together (MEL)

1. AWARENESS VS ACTION

Response Questions:

4. What role should government play in addressing the most serious threats to institutions and businesses located in Australia?
19. What private networks should be considered critical systems that need stronger cyber defences?
16. How can high-volume, low sophistication malicious activity targeting Australia be reduced?

Noetic believes it is important to recognise the disconnect between relative awareness and action on cyber security in Australia. Recent data suggests that senior executives[1] and SMEs[2] are improving their understanding of cyber risks. However, this trend of increasing awareness runs counter to the corresponding growth in the scale and severity of malicious cyber activity[3]. It is therefore clear that general cyber security awareness is on the rise in Australia, but appropriate behaviours and actions are not being implemented by the public and businesses to protect themselves against an evolving threat. With small business accounting for almost 98% of all business in Australia, and small to medium business (SMEs) employing almost 70% of Australia's workforce, contributing a total of 56% of total value added to Australian GDP, it is vitally important that appropriate actions are undertaken to protect them, their staff and customers[4].

For a large majority of these businesses and organisations "Human behaviour is the most significant weakness exploited in cybercrime"[5]. Unfortunately, a significant number of businesses continue to focus on technical solutions and overlook lower-cost measures to provide effective protection and mitigation strategies, such as the education of staff[4]. Whilst understanding of cyber security has increased, it seems that understanding of the protections and the potential severity of cyberattacks is not properly understood. Like 'Action 32'[5] in the 2016 Strategy, Noetic suggests that the government continue to focus considerable effort on growing awareness of cyber security. Whilst the 'Stay Smart Online Week' campaign was effective in reaching 6 million Australians, this target needs to be reviewed to eventually encapsulate *the majority* of Australians. Noetic proposes the government take on a larger role in raising awareness, implementing a national media campaign around cyber security, similar to the Aids campaign in 1987. The 'Grim Reaper' advertisement is not only iconic but, in conjunction with Australia's policy at the time, is attributed to driving the significant decline of Aids in Australia[6]. A similar national advertising campaign could employ the same 'shock' model used in the Aids campaign to better educate Australians about the effects of cybercrime, encouraging discussion and increasing awareness around the seriousness of the threat. This could go a long way in reducing the amount of successful high-volume, low sophistication cyberattacks on Australians.

Noetic also believes the government can do more to assist SMEs in their cyber security strategies, with 83% of SMEs expressing interest in a tool to help them tackle cybercrime[7]. We propose the government develop criteria to identify 'critical SMEs', comprising companies that are either fundamental to the government's operation and/ or hold valuable or sensitive data which could compromise national security if disrupted. Identified critical SMEs, by the nature and importance of their work, should be encouraged and supported to achieve increased levels of cyber awareness and protection. Noetic notes the government's intention to require certain companies to achieve compliance with the Protective Security Policy Framework (PSPF). We also note the difficulty many will face in achieving this, particularly funding the necessary measures. To assist attainment of increased cyber security posture the government could introduce a similar strategy to 'Action 17'[8] in the 2016 Strategy, by offering a form of funding support to critical SMEs to help them in the

[1] Source <https://www.minterellison.com/articles/2019-perspectives-on-cyber-risk>

[2] Source < https://www.smallbusiness.nsw.gov.au/sites/default/files/2019-07/Cyber-Aware-full-report.pdf>

[3] Source: <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-strategy-2020-discussion-paper.pdf>

[4] Source <https://www.asbfeo.gov.au/sites/default/files/documents/ASBFEO-small-business-counts2019.pdf>

[5] Action 32: Bring together and grow public and private sector cyber security awareness programs to make the best use of combined resources.

[6] Source < https://www.anzsog.edu.au/preview-documents/case-study-level-1/192-aids-grim-reaper-campaign-the-a-2006-90-1/file

[7] Source < https://www.smallbusiness.nsw.gov.au/sites/default/files/2019-07/Cyber-Aware-full-report.pdf>

[8] Action 17: Support small business to have their cyber security strategy tested by CREST Australia and New Zealand accredited providers.

development of robust and agile cyber security practices. This could be in the form of grants, tax deductions or co-payments.

Recommendations:

- The government take on a greater role in raising national awareness, with the implementation of a national cyber security media campaign.
- Identify 'critical SMEs' to government.
- Co-fund critical SMEs to support development of robust cyber security measures.

Result:

- A significant reduction in the number of successful high-volume, low sophistication cyberattacks on Australia.
- Increased protection of critical Australian SMEs.

2. UNDERSTANDING WHAT'S IMPORTANT

Response Questions:

1. What is your view of the cyber threat environment? What threats should government be focusing on?
17. What changes can government make to create a hostile environment for malicious cyber actors?
18. How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?

Noetic believes that an effective way to understand and prioritise what is important in increasing Australia's cyber security capabilities is through an enterprise risk management (ERM) lens. This approach is beneficial for several reasons. Firstly, it allows the government and organisations to better understand their approach to cyber risk reduction in terms of prevention and mitigation, and also by understanding the high pay-off critical controls they should apply.

Threat Assessment

One often seen failing of risk assessments is an inadequate threat assessment process. This flaw undermines the effectiveness of all that follows in understanding risk. Noetic believes that an accurate threat assessment is the cornerstone of building suitably robust cyber security settings, which are currently deficient in many organisations. If threat assessments are ill informed through poor inputs, low awareness levels, or simply inadequate, all prevention and mitigation controls implemented run the risk of being deficient in their protection, or inefficient in their over-protection.

We see this frequently and it reflects a generally low awareness of the likely threats and the process of a threat assessment. Without a full appreciation and articulation of the threats, organisations will fail to implement critical controls.

Similarly, we see organisations applying the conventional maturity-based approach in the management of cyber risk, whereby an organisation builds cybersecurity capabilities to reach a certain level of 'maturity'. Whilst this approach is useful for an organisation to begin the formulation of a strategy, it has the propensity to take on a 'mind of its own', and monitoring and other processes become an end in themselves, hindering real developments in the reduction of an organisation's cyber risks. Noetic contends inadequate threat assessments coupled with a focus on process and technical controls has led to an under appreciation of the importance of human factors and therefore impactful investment in important controls, such as effective employee education and training[9].

It is critical for organisations and government departments to be able to accurately produce suitable threat assessments. These will vary across government departments, SMEs and other agents in the economy. A valuable form of assistance the government could provide to improve threat understanding would be a capability uplift of the personnel who are currently producing threat assessments within businesses small and large. This capability uplift could be provided to both government personnel, companies and service providers who provide threat assessment services. While various standards of 'good practice' exist for threat assessment processes our experience is the standards are often poorly applied, with more emphasis on the process than the outcome. When poorly applied, the end result is a substantial negative cost for businesses and/ or the government. Whilst this approach does not indicate specific threats the government should be focusing on, it does provide a framework for prioritising threats, identifying the consequences and their prevention and mitigation measures. This allows for 'fit-for-purpose' threat assessments for different departments and organisations, tailored to their own circumstances.

Recommendations:

- Provide capability uplift to producers of threat assessments in government, business and service providers.

Result:

- The production of high-quality threat assessments across different departments and organisations helping them understand the threat events they face and strengthening Australia's cyber security.

Enterprise Risk Management and the Critical Control Approach

The Critical Control Approach (CCA) to enterprise risk allows the identification of appropriate prevention and mitigation controls and the mechanisms to manage and actively monitor those controls. We know from our work within Australia and globally that Black Swans are very rare.

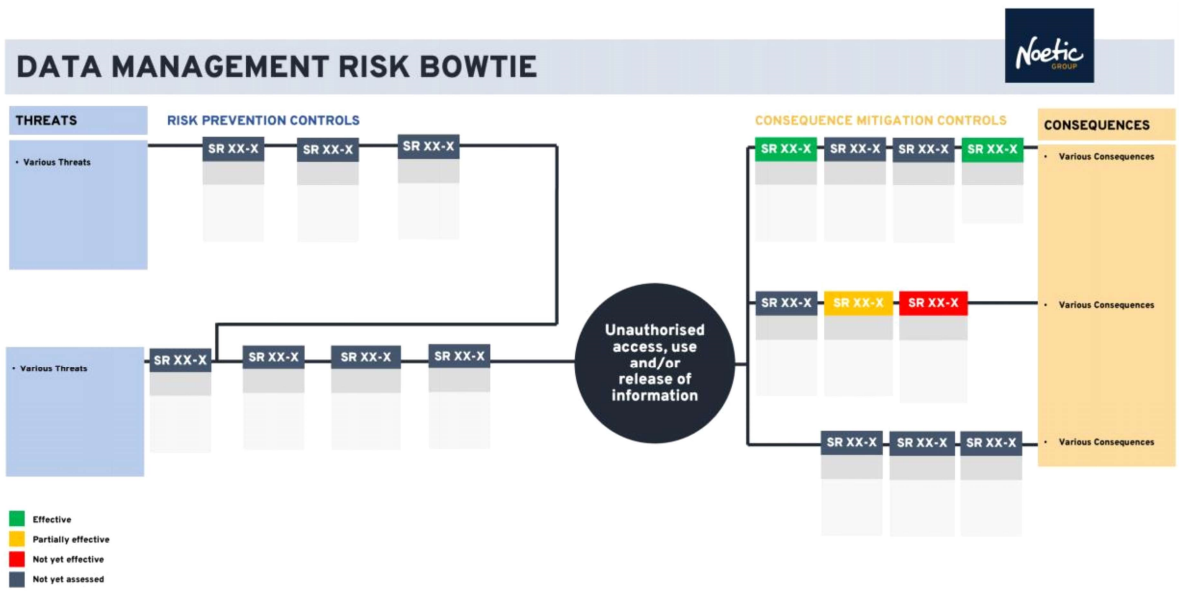
[9] Source <https://www.mckinsey.com/business-functions/risk/our-insights/the-risk-based-approach-to-cybersecurity>

Noetic's observation is that in most cases, bad things happen because known risks with known controls are poorly implemented.

We believe that applying an ERM lens to address cyber security is essential because traditional methods don't work and are time and again proven ineffective. For example, the generic risk matrix method, incorporating a consequence and likelihood rating, is at best misleading and at worse fatal. What is problematic about this approach is that it can deem material risks with catastrophic consequences but low likelihood to be within the risk appetite of organisations. This can have severe repercussions, as the threat events that lead to these risks becoming reality are accepted by an organisation, and adequate risk prevention and mitigation strategies are not properly implemented. This leaves organisations open to high consequence cyberattacks.

CCA counters this traditional methodology by using a systematic process to identify and analyse risks that might prevent an organisation from achieving its objectives, with emphasis on the aforementioned material risks[10]. CCA considers threats and consequences, and the controls required to prevent the risk event occurring and mitigate the consequences if it does. A key benefit of CCA is that the relationship between these components is clearly illustrated in a 'bowtie' diagram, as seen in Figure 1below. The graphical nature of a bowtie promotes a better understanding of the risk and serves as an excellent communication tool.

Figure 1.



One of the key strengths of using CCA is the formation of control profiles (see Annex A). Control profiles are the nitty-gritty of CCA and outline:

- the objective of the control;
- accountability for implementing and monitoring the health of the control (control owner);
- implementation actions and timeframe; and
- performance management metrics (KPIs).

[10] Material risks are those deemed as high consequence events regardless of the probability of their occurrence (often low).

Control profiles are regularly reviewed, positively validated for effectiveness and updated which is essential given the continuously evolving challenge of cyber security.

The CCA approach is primarily used by the resource sector in their enterprise risk management and process safety frameworks and is now becoming more widely adopted across government. Noetic has introduced the framework to several organisations, including the Department of Home Affairs and the Australian Financial Security Authority (ASFA). Noetic proposes that the government start to standardise the CCA approach in government departments to ensure proper cyber risk reduction and management. This would position the government as an exemplar in its understanding of cyber security risk management in Australia. This could also be extended to critical SMEs as identified in the previous section, to help strengthen their own cyber risk management procedures. These changes will result in an increasingly hostile environment for cyber adversaries and will also improve the processes for the identification and remediation of cyber risks.

Recommendations:

- Adoption of the Critical Control Approach (CCA) in government departments to ensure proper cyber risk reduction and management.
- Development of a Cyber Security Threat Assessment and Risk Management Approach tool kit for use by government and the private sector.

Results:

- An increasingly hostile environment for cyber adversaries, with a reduction in vulnerabilities.
- The improvement of processes for the identification and remediation of cyber risks across government, industry and business.

3. HOW EVERYTHING FITS TOGETHER – MONITORING, EVALUATION AND LEARNING (MEL)

Response Questions:

10. Is the regulatory environment for cyber security appropriate?
11. What specific market incentives or regulator changes should government consider?

Monitoring, Evaluation and Learning

A key component that Noetic believes can be improved upon from the 2016 strategy is the development of a more effective evaluation framework. The current framework evaluates each action of the 2016 strategy with a progression indicator, such as ‘progress’ or ‘complete’. Complementing these evaluations are ‘notes’ provided in the 2020 paper with additional

information regarding the specific action. While this goes some way to evaluating past strategy there are no key performance indicators (KPIs) for how effective the action has been in generating intended outcomes. Consequently, this provides no real indication of the success of the action itself. For example, 'Action 17' in the 2016 Strategy is:

"Support small business to have their cyber security strategy tested by CREST Australia and New Zealand accredited providers".

In the subsequent update in 2017 this action was labelled as 'progress' and in the 2020 paper it was labelled as 'complete'. Accompanying these evaluations are notes detailing how small businesses received co-funded grants for cyber security health checks. Whist this is a great initiative in assisting small business in cyber security protections, it provides no indication as to how effective the action has been in relation to improved cyber security outcomes. Clear outcome objectives and KPIs need to be established to assess how this action has impacted the small businesses that received the co-funded grant; the question as to whether receiving businesses took action to improve cyber protection or quantify a drop in successful cyberattacks compared to businesses that did not receive the grant remains unanswered? This is the key outcome of the action and a more fulsome evaluation framework would quantify its effectiveness. An effective evaluation framework also allows identification of an underperforming action to see what needs to change to achieve the desired outcome. Noetic believes this is fundamental to good policy implementation and every action needs to be incorporated into a strategy wide evaluation, monitoring and learning framework.

Recommendations:

- The establishment of a comprehensive evaluation, monitoring and learning strategy with key performance indicators (KPIs) for all actions in the 2020 Strategy.

Results:

- The ability to accurately analyse the effectiveness of the actions implemented by the 2020 Strategy, allowing for the identification and subsequent remediation of underperforming actions.

Regulation

In regard to the regulatory environment for cyber security in Australia, Privacy Principle 11 from the 1988 Australian Privacy Act notes that: If an Australian Privacy Principle (APP) entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information from:

- misuse, interference and loss
- unauthorised access, modification or disclosure.

This requires that most companies implement appropriate physical and information security systems to ensure that information held is protected. Whilst this is a good foundation for regulation, the rapidly changing cyber security environment requires new regulatory frameworks – what may have been reasonable in 1988 is unlikely to be fit for purpose in the current digital landscape.

More recently, The NDB Scheme, which came into effect on the 22 February 2018 and applies to organisations covered in the 1988 Privacy Act, made it compulsory for companies that suffer data breaches to notify the Office of the Australian Information Commissioner (OAIC). They must also directly inform the people whose information is exposed so they have the best possible opportunity to protect themselves from adverse effects. Whilst this builds on the foundations of the 1988 Privacy Act, Noetic believes more can be done to improve the regulatory environment in Australia.

When looking at the regulatory environment in the UK for cyber security there are multiple pieces of regulation that are specifically focussed on data protection and digital workings. A good example of this is the Data Protection Act 2018, which requires organisations to implement technical and organisational measures to safeguard personal data. While failure to implement these measures is not in itself a criminal offence, failure to comply with an enforcement notice resulting from failure of the above requirements that has resulted in an 'incident', is a criminal offence. While this regulation is similar to that outlined in Australia's Corporations Act 2001, which states that failure by a company to prevent, mitigate, manage or respond to an incident may result in breaches of the Act, businesses that are not classified as corporations have no requirement to mitigate potential risks, potentially leaving their business (and all of its information) vulnerable. It would therefore not be unreasonable to extend this regulation to critical SMEs and if successful, broader industry and business, to better prevent and mitigate cyber security threats in Australia.

Recommendations:

- An update to the regulation to include critical SMEs and broader industry and business.

Result:

- Standardised regulatory practices to ensure adherence to proper cyber security practices across Australia.

Concluding Remarks

The 2016 Cyber Security Strategy laid the foundation for protecting Australia against malicious cyber actors. The rapid pace of change in the cyberspace field requires that government continually review and update its cyber security strategy to stay one step ahead. With recent developments in cyberspace such as big data and artificial intelligence (AI), the landscape is set to change. These new technologies offer significant potential for Australia but also significant risk, as cyber adversaries adopt these emerging technologies. This response has sought to provide the government with recommendations on the development of the future 2020 Cyber Security Strategy (listed below) to help navigate the complexities of an ever-changing cyberspace. Noetic believes the adoption of these recommendations will greatly improve Australia's cyber security and will help protect Australians into the future.

Recommendations:

- The government take on a greater role in raising national awareness, with the implementation of a national cyber security media campaign.
- Identify 'critical SMEs' to government.
- Co-fund critical SMEs to support development of robust cyber security measures.
- Provide capability uplift to producers of threat assessments in government, business and service providers.
- Adoption of the Critical Control Approach (CCA) in government departments to ensure proper cyber risk reduction and management.
- Development of a Cyber Security Threat Assessment and Risk Management Approach tool kit for use by government and the private sector.
- The establishment of a comprehensive evaluation, monitoring and learning strategy with key performance indicators (KPIs) for all actions in the 2020 Strategy.
- An update to the regulation to include critical SMEs and broader industry and business.

ANNEX A:

Objective of the Control	*To ensure X we do Y.*	
Critical Control Actions List the critical actions that make the control work.	**Enabling Activities** List the activities that enable or support the Critical Control Actions.	**Verification checks** Describe the checks to verify the critical control actions and/or the enabling activities.
Program X		
Program Y		
Program Z		

Performance Measures		
Control Action	**Performance Targets**	**Intervention Trigger**
Program X		
Program Y		

Planning Information	
Location(s) where this function is performed	
Internal stakeholders	

Implementation Notes

Ownership, Reporting and Assurance

Role	**Classification/Title**	**Responsibilities**
Risk Oversight Forum		Responsibility and frequency
Risk Owners		
Control Owner		
Verification Activity Owner		

Noetic Group

Locked Bag 3001
Deakin West ACT 2600 Australia

Phone +612 6234 7777
Fax +612 6232 6515
www.noeticgroup.com