elevenM

Australia's 2020 Cyber Security Strategy

Submission

6 November 2019



Introduction

elevenM welcomes this opportunity to provide our perspective on the direction and maturity of Australia's cyber security strategy and capabilities.

As a passionately Australian company, we're emotionally invested in the safety and prosperity of this country, and recognise that national progress will increasingly depend on our collective ability to answer the significant challenges of the cyber domain.

Cyber security is critical for the Australian economy and its national security. In the last decade, the digitisation of Australia has continued at rapid pace and pervasively across all parts of the economy. The benefits of this digitisation are already being realised, and will continue to propel the economy forward in years to come.

At the same time, increased reliance on digital technology has brought additional exposure to a wide range of cyber risks. As the Government recognises in its discussion paper, cyber criminals and state actors are better resourced and more sophisticated than ever.

A strong and effective 2020 national cyber security strategy will not just help Australia mitigate risks in an increasingly perilous cyber threat landscape. It also represents a positive opportunity in a hyper-connected global economy. Resilient Australian companies that operate from within a digitally robust local ecosystem and regulatory environment will be highly attractive to individual consumers and businesses around the world – not least those in rapidly growing Asian countries on our doorstep.

elevenM's contribution to this conversation draws on our direct experience as cyber security and privacy practitioners. We have worked with many prominent Australian businesses and government agencies in the past few years, helping them understand and overcome digital risk challenges. In this paper, we highlight our insights and perspectives gained through these interactions. We hope it will be a constructive contribution to the development of the Australia's 2020 Cyber Security Strategy.

About elevenM

elevenM is a specialist privacy and cyber security consultancy.

We work with prominent brands, government agencies and start-ups, in Australia and across the world, to help them manage their digital risks and increase trust.

Our approach is to help clients monitor and protect data throughout the entire data lifecycle, by offering a holistic set of digital risk services. These include cyber security and privacy consulting, strategic communications and education.

Our team comprises leading practitioners with deep expertise, and spans multiple industries and jurisdictions.

1300 003 922

hello@elevenM.com

elevenM.com

Australia's cyber threat environment

Our perspective

Over the past few years, elevenM has worked with Australian organisations to manage the risks to their business posed by cyber threats. The threats faced by these businesses largely align to those seen by businesses globally.

Key threats including credential stuffing (enabled by large password dumps), phishing and spearphishing, malware (notably ransomware), and web-based attacks. Social engineering and payment fraud scams such as business email compromise have also been unrelenting, with the financial impacts potentially devastating for smaller businesses.

Supply chain attacks, in which attackers target software services used by a business, or their suppliers, have also become a more intense concern.

To inform their threat modelling and defensive activities, we observe organisations largely relying on generic, global threat intelligence, often supplied by overseas-based commercial providers.

Threat information that is contextualised for the Australian environment, and reflects threats specifically targeting Australian organisations is of high value but, in our view, difficult to access.

While threat information sharing networks (such as those operated by the Australian Government's Joint Cyber Security Centres) have matured since the 2016 Cyber Security Strategy, we see value in the Government issuing formalised threat reports and trend reporting focused on the Australian cyber threat landscape (building on the discrete advisories posted on cyber.gov.au).

The Australian Cyber Security Centre has in the past published threat reports reflecting the experiences of Australian businesses. On behalf of our clients, we'd encourage resumption of these kind of publications that coordinate data from Australian businesses and can be enriched with the Government's own actionable threat intelligence.

Recommendation 1

Enhance Government publishing of threat reports and provision of actionable intelligence based on the domestic threat landscape.

Managing cyber risk across the economy

In the course of our work with organisations of varying size and across different industries we've had the opportunity to observe emerging challenges for individual businesses in managing cyber risk, as well system-wide issues and patterns.

In the following section, we outline these observations, many of which align to the questions being explored by the Government's discussion paper.

A call for collaboration in the management of supply chain risks

Businesses today use hundreds or even thousands of suppliers for a multitude of services. The data and systems access given to suppliers in order to deliver these services is extensive, leading to a blurring of boundaries between organisations and their suppliers.

Many businesses are thus increasingly aware that their supplier's risk is ultimately also their risk. The recent incidence of major domestic data breaches as a result of a supplier compromise has further solidified this awareness. (For example, the 2018 breach of HR services provider PageUp and 2019 breach of property valuation firm LandMark White).

But despite this awareness, effectively governing the risk posed by a large number of suppliers is proving difficult and cost-prohibitive for most cyber teams. The sheer volume of time and

effort to gain true assurance over a multitude of suppliers is too onerous for many large organisations, let alone smaller businesses. Viewed from a broader, economy-wide lens, the present scenario in which the security capabilities of a single supplier are repeatedly assessed by each of its many clients suggests significant duplication of cost and effort.

We believe there is merit in a more coordinated approach to manage supplier risk. This could take the form of a national assurance scheme in which baseline security controls of supplier businesses are properly audited for design and operating effectiveness, and where results of this assurance may be shared.

Where a supplier's exposure within the ecosystem is so pervasive, the Government may even seek to take a more active role in assurance to mitigate the systemic risk.

We note developments in jurisdictions like Singapore, where legislation has been introduced to categorise certain digital assets as national critical infrastructure in an effort to mandate a level of cyber security across systems that significantly impact the wellbeing of their citizens.

Recommendation 2	Establish a national supplier assurance scheme that centrally assesses the security controls of supplier businesses and shares the results with participating businesses.

Scaling national efforts as an entire economy becomes more cyber aware

The 2016 Cyber Security Strategy played a commendable role in triggering awareness of the economic necessity of managing cyber security risk in a more connected digital world. There have since been a number of initiatives to better engage and support Australian businesses on this mission. These include the participation of many of Australia's largest companies in the Joint Cyber Security Centres (JCSC), which facilitate the sharing of threat information and

knowledge. Services and educational offerings for small businesses have also emerged in recent years, often from their own service providers in telecommunications or banking.

Campaigns and support for citizens and end users have been similarly enhanced, notably through cyber safety initiatives like Stay Smart Online and those run by the eSafety Commissioner, and the appointment of a Minister for Cyber Safety.

More recently, other sections of the economy have become attuned to the need to manage cyber risk. These include not only mid-tier companies but also larger enterprises in sectors that have not traditionally focused on cyber security risk. Many of these companies engage smaller consultancies – like elevenM – to assist them to understand their exposure and uplift their cyber security maturity.

Often, these companies do not have sufficiently large teams or dedicated cyber security capabilities to participate themselves in government initiatives such as those run by the JCSCs. At the same time, the advice and services now available for small businesses is often not appropriate to manage cyber risks for the scale and complexity of these larger businesses.

As the volume of businesses being serviced by cyber security consultancies grows, we believe there is merit in considering greater inclusion of these consultancies and service providers in government-run initiatives and knowledge-sharing activities (such as the JCSCs), so that the benefits of these initiatives can flow to these businesses.

We recognise (and accept) traditional reticence to involve commercial vendors in government-supported initiatives.

However, it is also the case that many of these vendors and service providers – while commercially motivated – are passionate about reducing the risk of their clients and supporting a more secure and resilient Australian ecosystem. Perhaps models could be considered in which service providers are included on the basis of sponsorship by Australian businesses.

The growing number of businesses supported by these cyber service providers is a key change since the 2016 Cyber Security Strategy and merits, we believe, a discussion about how the government engages all active participants to manage cyber risk in the economy.

Recommendation 3	Foster greater engagement of cyber security consultancies and service providers in national cyber initiatives (such as those run by the JCSC), to support sectors of the economy and businesses that manage their cyber risks via those providers.

Keeping up the momentum on attracting cyber security talent

Addressing the cyber security skills shortage was a key objective of the 2016 Cyber Security Strategy.

While there continues to be a global shortage of cyber security professionals, in the wake of the 2016 Cyber Security Strategy there have commenced a number of commendable initiatives to grow the pipeline of cyber security talent. These include industry-sponsored tertiary courses, vocational training programs and, more recently, programs to embed cyber skills into the school curriculum.

Anecdotally, we observe a growing number of graduates and interns with a sharpened interest in cyber security, and hope that these are the green shoots for a healthier pipeline of young, domestic cyber security talent.

At the same time, many businesses continue to struggle in identifying and attracting high quality cyber security talent into senior, strategic roles.

Vacancies in the Chief Information Security Officer (CISO) position are a particular thorn in the side. We are aware of major organisations that have struggled to fill CISO positions for extended periods, with the domestic pool of candidates with sufficient experience for the role found to be shallow.

Many businesses are thus forced to operate without this role entirely, have it performed in a part-time or acting capacity by another executive, or to outsource it.

The impact on Australia's cyber resilience resulting from organisations struggling to fill these strategic security roles shouldn't be underscored. When occupied with well-qualified candidates, positions like the CISO are a true catalyst for maturing the security of our national companies. They achieve critical outcomes including, but not limited to, "turning on" cyber security awareness of boards and the entire business, obtaining funding for vital security uplift programs, instilling a culture of cyber security across an organisation, and inspiring and marshalling cyber security teams to

better meet the demands of a fast-evolving threat landscape.

Under the 2020 strategy, as part of the next phase of its focus on the skills landscape, we recommend a focused discussion on helping Australian businesses address gaps in this critical portion of the cyber security workforce.

Consideration might be given to how Government could promote the attractiveness of Australian companies for the international cyber security workforce, particularly through its international relationships (e.g. the Five Eyes).

Longer term, prioritising the appointment (and appropriate remuneration) of roles such as the CISO in government agencies could also be a driver and lure for this talent into the domestic marketplace (in addition to having the effect of improving cyber risk management in the government sector).

Recommendation 4	Ensure skilled migration schemes effectively support luring of strategic cyber security professionals to Australia from global talent pools.
Recommendation 5	Explore opportunities for rotation schemes for strategic cyber security professionals between government agencies and businesses within Australia's partner nations, such as the Five Eyes.

A stronger national voice on cyber security, privacy and data issues

As we outlined in the introduction to this submission, cyber security is a critical national issue with implications for both the economy and national security.

The mission encompasses a great deal and requires contributions from a great many – not least committed actions by governments and industry, effective

regulatory frameworks, continuous engagement of Australian citizens and the maintenance of fruitful international partnerships.

To catalyse and activate these many players, and to cohesively unite the many cyber security programs and initiatives underway and ensure they align to our national priorities, we require a strong and persistent national voice on cyber security. Industry will also benefit from a single senior government figurehead to whom it can raise cyber security concerns and issues.

Ideally, we believe this translates into a designated voice and responsibility for cyber security within the Government's ministerial portfolios. Such a ministerial role was created under the 2016 Cyber Security Strategy, however appears to no longer exists.

At present, cyber security is an accountability for the Minister for Home Affairs. Home Affairs is a broad and complex portfolio, also dealing with issues including immigration, organised crime, terrorism, espionage and lawful interception. Given this spectrum of issues on which the Minister for Home Affairs must communicate to the nation, and the weight of each, we feel cyber security is at risk of being underserved or associated primarily with national security (versus economic prosperity) in the minds of most citizens.

More must also be done to unite cyber security policy and initiatives with contemporaneous digital issues of privacy, disinformation and data governance and sharing. These issues, and the risks they represent, are fully intertwined in the modern digital economy.

We work with a number of mature businesses who increasingly recognise the need to manage their digital risks holistically, and to ensure that programs that govern security, privacy, and ethical and efficient use of data work hand in hand.

We propose that a similar evolution of the national conversation started through the 2016 Cyber Security Strategy would be logical. In doing so, Government can help less mature businesses contemplate the overlap of these issues within their own operations, and also foster an improved civic dialogue in which Australian citizens better understand the intersection of these issues as consumers.

Recommendation 6	Appoint a senior Government Minister with dedicated responsibility for cyber security.
Recommendation 7	Review policy development forums and processes to ensure that cyber security, privacy and data-related considerations are included in the development of policies for any of these domains.

Conclusion

A cyber future marked by collaboration, leadership and goodwill

The 2016 Cyber Security Strategy was well-thought out and set out a positive direction for Australia's digital economy.

We're aware that many of the programs and initiatives emerging from the strategy have had a positive impact. It's also apparent that in the last four years there has been a broader and more inclusive dialogue about cyber security and its importance for Australia. This is all good news.

Yet as the digitisation of the Australian economy continues, and technologies including artificial intelligence and the Internet of Things become more embedded, the task of getting cyber security right has only become more important.

Four years having passed since the previous strategy, an appropriate time to reflect on whether we are indeed getting things right and what may have changed.

In this paper, we have shared some of our insights to those questions. What is clear to us is that fundamental challenges continue to exist that necessitate more coordination, greater national leadership, and better marshalling of the natural goodwill in the sector to create a more secure and resilient nation. A 2020 Cyber Security Strategy is the ideal vehicle to pursue and achieve each of these outcomes.

elevenM anticipates that many of the solutions likely to be proposed by the new strategy will require a collaborative approach. We welcome any opportunity to either expand on our ideas in this submission, or to participate in any other way in the development or execution of Australia's 2020 Cyber Security Strategy.

Please contact us at hello@elevenm.com.

Thank you.