Apollo Secure Pty Ltd
Suite 2, Level 4, 109 Pitt Street
Sydney NSW 2000
15 April 2023

Re: 2023-2030 Australian Cyber Security Strategy Discussion Paper

Introduction

As an active member of the Australian cybersecurity community, we welcome the opportunity to participate in this Cyber Security Strategy Discussion Paper. We see this as an important step in achieving consensus around developing an effective cyber strategy for Australia now and into the future. We commend the bold vision set by The Hon Clare O'Neil MP, for Australia to become the world's most cyber secure country by 2030 and agree that this will require significant effort from government, industry and the community working together with a clear and unified strategy.

The coordinated effort required to achieve this ambitious goal will include a range of measures from policy reform and grass roots education to investment into the cyber ecosystem and community programs.

Apollo Overview

Apollo works with small businesses to help improve their security posture and build trust with their customers and partners. We understand that security isn't top-of-mind for most small business owners and the 'she'll be right' attitude doesn't always help them adequately prepare to defend themselves. We developed our platform to be as simple and automated as possible so they can achieve security outcomes without the usual complexity and cost.

We work with partners and industry bodies such as AustCyber and Investment NSW to help make cybersecurity more accessible to small businesses and therefore reduce cyber risk for the broader community.

Our Response

As our expertise is centred around cybersecurity for Small-to-Medium Businesses (SMBs), we have focused our submission on how Australia can work towards reducing risk for SMBs. We will therefore seek to address some specific questions detailed in Appendix A of the discussion paper in that context.

The structure of our response will cover some of the challenges that SMBs face in their cyber preparedness and include recommendations for both SMBs and the national bodies that represent cybersecurity in Australia. This will include the standards and incentives that we believe will be required to realistically improve SMBs' security posture. Our view is that an essential part of Australia becoming the most cyber secure nation by 2030 (any beyond), is to improve the security

posture of SMBs with a pragmatic and affordable framework. A coordinated collaboration between all stakeholders, including the development of a meaningful framework for SMBs, will maximise the likelihood of a successful outcome for the economy at large.

SMB cybersecurity preparedness – characteristics and challenges

The importance of SMBs to the economy and the growth in cyber attacks

Of the 2.4 million businesses in Australia, 98% are small businesses with less than $10m turnover[1]. Small businesses are the backbone of the Australian economy – driving innovation, creating jobs and contributing to economic growth. SMBs account for around 35% of the country's GDP and employ approximately 44% of the total workforce[2]. The sector is diverse, ranging from sole traders and micro-businesses to mid-sized organisations and encompasses a broad range of industries including retail, construction, trade, professional services and hospitality to name a few.

There is an increasing dependency on technology and communications for all types of SMBs. Accelerated by the COVID pandemic, many SMBs have transitioned to remote work using various online platforms and services such as remote access, video conferencing, cloud services and collaboration tools. The pandemic has underscored the importance of digitization in all industries and has highlighted the need for SMBs to ensure business continuity by improving their online processes and infrastructure.

In parallel with this online adoption, there has been a rise in the number of cyber attacks, including increasingly sophisticated phishing attacks and a sharp rise in ransomware[3].

- Over 76,000 cybercrime reports (one every 7 minutes in 2022) which is an increase of 13% from the previous financial year.
- Over 25,000 calls to the Cyber Security Hotline, an average of 69 per day and an increase of 15 per cent from the previous financial year
- A rise in the average cost per cybercrime by 14% (i.e. $39,000 for small business, $88,000 for medium business).
- An increase in financial losses due to business email compromise to over $98 million - an average loss of $64,000 per report.

---

[1] The Australian Small Business and Family Enterprise Ombudsman 2021

, Contribution to Australian Business Numbers,

[2] Small business sector contribution to the Australian economy

https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1920/SmallBusinessSectorAustralianEconomy

[3] The Australian Cybersecurity Commission (ACSC) responded to almost 70,000 cyber crime reports in the FY21/22

https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022

SMBs underestimate cyber threats and are poorly prepared to respond to cyber attacks

Unfortunately, many small businesses believe that it is only larger organisations that are at risk from cyber attacks. It appears that unless cybersecurity controls are included by default as part of an IT solution, many SMBs do not realise the potential risks posed to their business and take the necessary steps to protect themselves.

Even if an SMB accepts that the risk of a cyber attack is real, they face many challenges in being prepared to prevent it. For example, the ACSC small business survey in November 2020[4] concluded that:

- Almost half of SMBs rated their cybersecurity understanding as 'average' or 'below average' but had poor cybersecurity practices.
- SMBs underestimate the impact of a cyber incident.
- SMBs outsourcing IT security believe they are better protected than they really are.
- SMBs lack dedicated IT staff and that cyber security has to compete for time and other resources with multiple demands.
- Business owners often fail to identify weaknesses in security practices and know they are struggling, but do not know where to begin to remedy their security posture.
- There was a lack of planning to enable SMBs to properly respond to cyber incidents.
- 1 in 5 SMBs did not know the meaning of the term "phishing".
- Almost half of SMBs reported they spent less than $500 on cybersecurity per year.

SMBs are a major supply chain risk to enterprise and government organisations

Small businesses are often seen as the 'weak link in the chain' with cyber criminals often targeting them to gain access to larger organisations or government networks that they're connected to. Beyond the supply-chain risk they pose to larger organisations, most SMBs process some form of personal information[5], making cybersecurity a significant risk for them and their customers. While SMBs traditionally haven't represented the same level of risk as larger organisations, due to the hyper-connected nature of the internet, they now have access to a similar amount of sensitive data through integrations to larger partners and therefore have a similar level of risk as larger companies.

---

[4] Results from the Australian Cybersecurity Centre Small Business Survey 2020 https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/small-business-cyber-security

[5] The term personal information refers to information that if stolen or lost, may lead to an SMB incurring significant cost and involve potential legal repercussions.

https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information

PageUp Case Study[6]

One notable case study from Australia that demonstrates how SMBs can pose a significant supply chain risk to larger organisations is the 2017 data breach at Australian human resources company, PageUp.

PageUp is a provider of HR software and services to many of Australia's largest companies including banks, government agencies and retailers. In June 2018, the company disclosed that it had suffered a major data breach that potentially exposed the personal information of millions of job candidates and employees at its client companies. An investigation revealed that the breach was the result of a cyberattack on PageUp's systems, which had been compromised through a vulnerability in the company's website. The investigation also found that the attackers had gained access to the personal data of individuals stored on PageUp's systems, including names, addresses, email addresses and employment details. One of the key factors in the breach was that PageUp's system was integrated with those of many of its clients, including some of Australia's largest corporations, making it a critical component of their supply chains. As a result, the breach had a significant impact on these organisations, exposing them to reputational damage and potential legal liability.

Recommendations for SMBs to improve their cybersecurity posture

People, processes and technology

The core cybersecurity areas that need to be addressed by SMBs are around people, processes and technology (and how they intersect). For example, data privacy is a critical aspect of cybersecurity where people, process and technology must be coordinated to avoid a crippling data breach. For businesses to comply with regulatory and legal requirements such as the Australian Privacy Act, a culture of compliance must be driven by management and include defined business processes such as access controls to securing systems that store personal data. Too often, SMBs avoid addressing 'the low hanging fruit' of a good cyber posture by mistakenly believing that it is a purely technical endeavour and one that is prohibitively expensive. However, implementing and maintaining cybersecurity measures for SMBs doesn't have to start with technical investment and does not always have to be expensive. There are various measures that can be implemented without requiring a significant or complex technical investment.

[6] PageUp Case Study
https://www.abc.net.au/news/2018-06-06/australian-data-may-be-compromised-in-pageup-security-breach/9840048

Creating cyber awareness and a culture of preparedness

85% of data breaches are caused by human error, according to a Stanford University study from 2020[7], which is why security awareness is often considered the biggest opportunity for reducing cyber risk with minimal investment and limited technical effort.

It is therefore necessary to establish a culture of security awareness within organisations via training programs that educate staff on how their behaviour can affect the entire organisation. For example, it is essential that all staff understand how threats such as social engineering work, the guidelines for using their own devices, what the company policies cover and other basic security measures. SMBs must also provide specialised training to staff members dedicated to IT and cybersecurity. This shift must be management-led and company directors and senior management but be identified to take ownership of the organisation's cyber posture.

Establishing company policies and procedures

Like other company policies such as OH&S policies and anti-discrimination policies, security policies outline the company's stated position on how staff should act in carrying out their duties and help staff understand what to do and what not to do while at work. It's important that staff are aware of these policies and that people in particular roles such as management and IT staff are following the procedures outlined in those documents. In terms of process, establishing documented and regularly tested plans with clearly defined roles and responsibilities for responding to incidents such as phishing attacks, data breaches or natural disasters is crucial. Policies should also cover topics such as resetting all default passwords on systems and enforcing the use of strong passwords. These things are not technically challenging or necessarily expensive, but small businesses need to be made aware of these measures so they can document them and better protect themselves against an attack.

Implementing technical controls against cyber threats

From a technical perspective, firewalls, antivirus protection, encryption access control and secure backups are some of the technical controls SMBs should consider to ensure effective cybersecurity. Although these controls will often require technical skills to implement, they are often either free or quite cost effective for SMBs with a small number of users. If SMBs struggle to manage this themselves there are effective solutions offered by the major cloud providers (i.e. AWS, Azure, Google) as well as Managed Service Providers (MSPs) to help technical decision-making and implementation.

Community campaigns to increase cyber awareness

[7] Stanford University and Tessian, The Psychology of Human Error, 2020. https://www.tessian.com/research/the-psychology-of-human-error/

There are a number of initiatives that could immediately reduce the risk profiles of SMBs. These include educating the SMB sector through broad awareness campaigns that clearly state the issues facing businesses that ignore cybersecurity threats, as well as the opportunities and benefits that come with improving their cyber posture. Raising awareness is best done in partnership with business representative organisations such as ACSC and AustCyber to educate business owners, managers, employees and shareholders on cybersecurity issues. The content of the campaigns should be aimed at the needs of SMBs and focused on helping them understand cybersecurity threats and how they can protect their businesses. It is also suggested that the methods of implementation should be carefully selected and tailored to each business sector. The effectiveness of these campaigns should be measured through regular surveys, feedback from SMBs and analysis reports of cybercrime incidents.

Improve and evolve guidelines and tools for SMBs

For SMBs with limited resources and knowledge of cybersecurity, the path to implementation can be unclear. Many SMBs are not aware of specific standards or methods for implementing security and privacy measures. To bridge this gap, it's important for the government to provide clear and structured implementation guidelines including easy-to-use tools and templates. These resources should include realistic and specific examples, simple language that is easily understood, and be tailored to the characteristics of SMBs, including the criticality of the information processed, industry, and dependence on information and communication technology (ICT). To ensure the effectiveness of these resources, it's recommended that public-private collaboration take place with SMB representative bodies, relevant public sector organisations and cybersecurity consultants. This collaboration will help to define and refine the guidelines, procedures and standards, ensuring that they are both relevant and useful to SMBs.

With around 2.35m small businesses in Australia, most of which have limited budgets and resources, it’s important to provide automated and streamlined processes to provide sufficient coverage in an efficient manner. This can also include things such as access to cyber self-assessment tools, where SMBs can answer a set of simple questions to generate a tailored report with clear actions to improve their security posture.

Implementing an Australian Cyber Standard for SMBs

The improved regulatory frameworks for corporates and government departments are clearly a positive step in improving overall cyber resilience, and a harmonised standard for SMBs would be a major win for the Australian economy, but it is unrealistic to expect SMBs to meet the same level of compliance against the same set of standards. A national standard for SMBs is essential given the ubiquity of SMBs across our economy and the fact that SMBs are often a supply chain risk for their larger enterprise and government partners. Although there are many cybersecurity standards available, SMBs are often hesitant to adopt them. This is mainly due to the existing standards (which

are designed for larger organisations and government departments) being too onerous for SMBs who have simpler systems and processes which present lower severity risks. Further, there is no compelling reason for SMBs to comply with recognised standards, because there is no regulatory requirement and no industry pressure to do so. A new approach is needed, one which actively incentivises SMBs to participate alongside a genuine understanding that they can benefit commercially from aligning to an attainable, affordable standard. It is therefore imperative to implement a standard designed specifically for SMBs, similar to approaches taken by other countries.

To avoid re-inventing the wheel, it is advisable that any new standard for SMBs be aligned to an existing standard such as ISO27001, which is often regarded as the global gold standard in cybersecurity. This ensures that the new SMB standard is built on the right foundations and also allows growing small businesses to build upon the controls implemented for the new SMB standard as they progress along their journey to something more comprehensive like ISO27001 down the track. It is therefore envisaged that an 'ISO27001 Lite' standard be developed which takes the 'low hanging fruit' from the full ISO27001 standard to derive a new standard that can achieve the most security outcomes for minimal investment in time and money.

The UK Cyber Essentials program

The Cyber Essentials[8] program, developed by the NCSC in the United Kingdom was developed to be a relevant and achievable framework for SMBs. It requires participating businesses to undergo an independent assessment of their security measures and the program incentivizes them to take cybersecurity seriously and make it a priority. The Cyber Essentials standard covers 5 key areas: firewalls, secure configuration, security update and management, access control and malware protection. Participation incentives include a recognisable certificate of achievement and subsidised cyber insurance cover. The success of the Cyber Essentials program in the UK can be seen in the high adoption rates among businesses of all sizes and the positive impact it has had on raising awareness of cybersecurity and promoting a culture of security within organisations. For example:

- According to the UK government, as of March 2021, over 40,000 UK businesses had been certified under the Cyber Essentials scheme since it was launched in 2014.

- A survey conducted by the Federation of Small Businesses (FSB) in 2018 found that 23% of small businesses had experienced a cyber-attack in the previous 12 months. However, of

[8] 1 About Cyber Essentials, National Cyber Security Centre UK
https://www.ncsc.gov.uk/cyberessentials/overview

those businesses that had implemented Cyber Essentials, only 4% had experienced a cyber attack.

- In a case study published by the UK government, a small IT services company called Computing Dynamics reported that achieving Cyber Essentials certification had helped them to win new business, as it provided assurance to clients that they took cyber security seriously. The company estimated that achieving certification had resulted in an additional £50,000 of revenue.

- A survey conducted by CyberSmart in 2021 found that 75% of UK small businesses believed that achieving Cyber Essentials certification had helped them to improve their cyber security posture.

Overall, these statistics suggest that the Cyber Essentials program has been very successful in helping UK small businesses to improve their cyber security and protect themselves against cyber attacks. It has also helped to create a common language around cybersecurity, making it easier for businesses to communicate with each other and with their customers about their security posture.

Although Cyber Essentials is a good program for SMBs and has achieved a lot of success, it does fail to cover some of the critical steps for a sound cybersecurity framework including security policies, staff training and vulnerability assessments, which are required by most other standards and deemed to be foundational requirements even for small businesses. It could also be more directly aligned to a global standard such as ISO27001 for the reasons mentioned above.

The Essential Eight is not designed for SMBs

It may seem like an obvious approach for the government to adopt the Essential Eight framework for SMBs, because it already exists as an ‘entry-level’ framework in Australia and sounds like a straightforward standard with only 8 requirements. However, it was not designed for SMBs and it may be a case of trying to force a square peg in a round hole.

The Essential Eight was initially developed for government departments back in 2017 (having also since been adopted by corporate entities who are servicing government departments) and is focused primarily on Microsoft Windows-based networks and devices which are centrally owned and managed. MacOS adoption has increased sharply since 2017, particularly in the SMB and consumer spaces, with entire industries such as design and software development running almost exclusively on MacOS, leaving much of the Windows-based Essential Eight being redundant for many SMBs. Further, most SMBs have a higher proportion of staff using their own devices (BYOD) and the pandemic has amplified this behaviour with people working from home on their own computers more than ever. This leaves most of the Essential Eight requirements being out of reach for SMBs because it’s hard for them to enforce policies on devices which they don’t own or control and which aren’t sitting within a corporate network.

Despite the name suggesting there are only 8 requirements to meet, the reality is that there are actually 8 *categories* of requirements and up to almost 70 individual requirements within those categories at the highest maturity level. This is not far off the 93 controls included in the comprehensive ISO27001 standard, which is deemed to be out of reach for most small businesses.

There is also quite a varied level of complexity across the Essential Eight requirements, many of which are too rigorous for most small businesses to consider. For example, even at Maturity Level One (a basic maturity level), organisations need to be running vulnerability scans of their internet-facing services every day, which is quite a high level of sophistication and something beyond the scope of many larger organisations (who would often only run vulnerability scans perhaps a few times a year), let alone SMBs who don't have the technology or operational capability to meet this requirement.

The Essential Eight is also not directly aligned to a global standard such as ISO27001. Although there is some overlap between them, meeting the Essential Eight would leave some major gaps and also require some work that wasn't on the path towards ISO certification.

Some obvious omissions from the Essential Eight are security policies and staff training, which are both deemed to be critical requirements under most other standards. There is no mention of organisations needing to develop company policies to establish an internal framework around cybersecurity and security training to ensure staff are adequately armed with the knowledge to protect the company from cyber threats – something often considered to be the greatest risk to a data breach and perhaps the biggest and easiest opportunity to improve a business's security maturity.

There are certainly some good aspects of the Essential Eight standard – the tiered maturity model provides a level of flexibility along an organisation's cyber journey, and there are plenty of learnings to be applied to an SMB standard, but a considered approach needs to be taken to ensure that the requirements of any new standard are relevant for SMBs and that the bar isn't set too high for them, to a point where they don't bother doing anything at all. Cybersecurity is a journey and it's important that small businesses have an achievable first step to work towards along that journey to get them secure and compliant.

A Cybersecurity maturity journey towards recognised standards

In partnership with national cyber representative bodies such as ACSC and AustCyber, as well as the private sector, a set of requirements should be developed with flexible maturity levels that empower all SMBs to achieve important milestones dependent on factors such as their size, sector and function. While it is hard to develop a 'one-size-fits-all' approach to cybersecurity, there are some fundamentals that will always apply and are affordable to implement. As an SMB's risk profile evolves over time (in relation to their size, sector, access to sensitive data etc) they can choose to progress up through the maturity levels and onto recognisable certification paths such as ISO27001.

An example framework

A lite cybersecurity framework for SMBs could include something like the following requirements:

Requirement	Maturity 1	Maturity 2	Maturity 3
1. Malware Protection	Basic	Moderate	Advanced
2. Content Filtering	Basic	Moderate	Advanced
3. Firewalls	Basic	Moderate	Advanced
4. Password Management	Basic	Moderate	Advanced
5. Multi-Factor Authentication	Basic	Moderate	Advanced
6. Mobile Device Management	Basic	Moderate	Advanced
7. Physical Security	Basic	Moderate	Advanced
8. Vulnerability Scanning	Basic	Moderate	Advanced
9. Data Backup & Recovery	Basic	Moderate	Advanced
10. Data Encryption	Basic	Moderate	Advanced
11. Security Policies	Basic	Moderate	Advanced
12. Staff Training	Basic	Moderate	Advanced
13. Access Control	Basic	Moderate	Advanced
14. Compliance with Regulations	Basic	Moderate	Advanced

The specific requirements could be reviewed and updated in consultation with representative bodies and industry experts, and the specific details under each maturity level would need to be defined in collaboration with multiple parties. The terminology used here is deliberately quite basic and broad to allow business owners to understand it and also to avoid being tied to current trends in products and solutions which may become outdated, but it is appreciated that some of the language could be updated to align to standards and more modern terminology. As an example, the Antivirus requirement could look something like this:

Malware Protection

Anti-malware software provides protection against viruses, malware, phishing and other attack types and it's important to have this in place to protect company systems and data.

Maturity Level 1

- Businesses need to have antivirus software installed on all laptops, desktops and servers which have access to company information, including laptops owned by staff and contractors who use it for work purposes.
- Auto-updates need to be enabled to get the latest signatures on all devices.

Maturity Level 2

The Maturity Level 1 requirements, plus:

- The software needs to be centrally-managed to ensure updates are being applied to all devices and to provide centralised reporting and alerts.

Maturity Level 3

The Maturity Level 1 and 2 requirements, plus:

- Businesses need to have advanced endpoint protection software installed on all laptops and desktops which have access to company information, including laptops owned by staff and contractors who use it for work purposes.
- Endpoint protection includes intrusion prevention.
- Endpoint protection includes application control.
- Endpoint protection is configured to automatically quarantine or remove any identified threats.
- Endpoint protection includes behavioral analysis to detect suspicious activity.

Conclusion

There is no silver bullet with cybersecurity and for Australia to be the world's most cyber secure country by 2030, there will be a number of initiatives required across the public and private sectors under a well-defined, unified strategy. With SMBs making up such as significant part of the Australian economy and often being perceived as 'the weakest link in the chain' when it comes to cybersecurity, it is imperative to develop a new national framework designed specifically for SMBs to give business owners the guidance they need to improve their security posture and to allow them to work through a defined standard to minimise the risk of a security incident and allow them to prove their cyber resilience to their customers and partners with an achievable and affordable certification.