2023-2030 AUSTRALIAN CYBER SECURITY STRATEGY

CYNCH SECURITY SUBMISSION

This page is left intentionally blank

Responses

Introduction

Australia's small businesses face unique challenges when it comes to building cyber resilience due to significant resource constraints. Costs and disruption from cyber attacks can disproportionately impact small businesses compared to larger, well-resourced victims. Low awareness of cyber risks among many small business cohorts further hampers their ability to proactively manage these growing threats.

Building cyber awareness and resilience among small businesses presents a key opportunity to grow Australia's cyber sector. By supporting Australian small businesses to develop greater cyber resilience, Australia's economy and national security will also grow.

Cyber Fitness for Small Business

Cynch Sec Pty Ltd (Cynch) is a proud Australian cyber security startup, established in 2018. The team's mission is to help small business owners avoid having a cyber incident becoming the worst day of their working lives. They provide SaaS and consulting solutions to more than 1,000 small businesses and their enterprise and government clients, helping them build Cyber Fitness in and around critical supply chains.

Question 1

What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

While Australian small businesses represent more than 97% of Australian businesses, almost no investment into the cyber security of this critical sector has been made. To become the most cyber secure nation in the world, this needs to change.

While awareness raising and sharing of simple "tips and tricks" may be a necessary starting point, small businesses, the back-bone of the Australian economy, deserve more than a simplified afterthought.

Elevating the importance of cyber security amongst small businesses in the Strategy will establish a trusted foundation onto which a cyber secure economy can thrive, and create opportunities to grow the cyber security industry and workforce needed to bring the most cyber secure nation to life.

Continued exclusion of small businesses from regulation, investment and capability building may lead to cyber secure government and big businesses, but leave the small business sector behind, exposed and vulnerable to a risk they are unable to manage.

Specific recommendations on how to approach this outcome within the Strategy are discussed in our responses to the following questions.

Question 2

What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?

a. What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?

One of the most challenging aspects of managing cyber risk within the small business sector is keeping up with the rapid evolution of the threat landscape. The context businesses operate within shifts on a weekly basis, far more frequently than any legislation or regulation is able to be updated.

Legislation that makes it clear what penalties apply to businesses choosing to ignore the risk, placing the community in harm's way, may be effective, however continued carve outs for small businesses undermines this as an effective mechanism. All businesses should be considered within legislation, not just those that will find meeting expectations easy.

Regulation in certain areas (e.g. Critical Infrastructure) has been somewhat more effective at guiding attention towards treatment of cyber risk amongst associated small businesses, however a lack of right sizing of regulations towards the context of small businesses creates a significant barrier to broader adoption.

Improved guidance towards the implementation of regulations within a small business context would enable every business to do the right thing.

Ideally though, improvement should be made across all mechanisms.

b. Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

As recent incidents have demonstrated, broader community expectations suggest that customer data and 'systems' should also be protected, particularly where there is an aggregated risk to harm. In our experience working within the Critical Infrastructure ecosystem, there is little of no difference in the way cyber risks within Critical Assets, Customer Data and Systems is managed as teams are often too constrained to tailor their approach to a given context.

This suggests extending the definition to include customer data and systems may not present a significant impact to organisations, however a better outcome may be the consideration for how to determine the criticality of a given asset and an acceptable level of associated risk. This could then be leveraged in downstream considerations for smaller, less 'risky', suppliers participating within the Critical Infrastructure ecosystem.

"Willing to just give up"

The Critical Infrastructure supply chain relies on the products and services of thousands of small businesses. In working with many of these key suppliers, we have heard time and again how burdensome 'standard' assurance processes are. An individual contract could represent more than 50% of revenue for a small supplier, yet it is not uncommon to hear statements such as "*Most of us that went through it were willing to just give up*".

Changes to SoCI and other legislation need to account for small business involvement or risk locking them out altogether.

c. Should the obligations of company directors specifically address cyber security risks and consequences?

We have observed a significant uptick in the number of smaller businesses actively seeking to understand cyber risk as part of their broader risk management activities. It is clear in these discussions that company directors are already concerned about the consequences of a cyber incident, however their obligations to ongoing management of the risk is not yet well understood.

Greater clarification of these obligations to company directors is likely to improve the interest amongst these businesses in more actively managing cyber risk and should therefore be explored.

Not what the board wants

Cynch recently worked with a small training business representative looking to provide their board with a cyber risk update. Through discussions it became apparent that the board was not looking for a cyber risk report, instead they were looking for validation that the decisions they'd already taken were correct and confirmation there was no more investment needed. We do not expect this board to revisit their cyber risk until an incident occurs.

d. Should Australia consider a Cyber Security Act, and what should this include?

While existing legislation within the Privacy Act and SoCI Act provide clarity to many large businesses, there are few small businesses for which these laws directly apply. A separate Cyber Security Act presents a significant opportunity for setting out the baseline expectations for cyber security every business in Australia (including small businesses) should be following. This should be developed in such a way that the broader community can base their trust in Australian businesses digitally.

As noted, attempting to prescribe specific measures will quickly become outdated, instead focus should be given to outlining practices all businesses should be adopting to effectively manage cyber risk.

e. How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?

While we have direct anecdotal evidence of the impacts of regulatory changes to small businesses, we have seen no public discussion of this issue. The introduction of additional obligations through programs such as DESE's Right Fit for Risk (RFFR), were catastrophic for smaller providers, with many suggesting to us that they were considering shutting down or simply stopping their involvement in delivery of government services as a result. Monitoring and sharing data on small business participation in these ecosystems would be a critical part of understanding the burden such changes creates.

Many small businesses are starting from scratch with regards to cyber risk management and as such will be disproportionately impacted by any broad regulation introduced. Tax incentives and/or grants directly aligned to adoption of regulations should be considered, particularly in those areas already struggling to maintain an operational workforce. Take up of incentives can provide insight into both the additional burden as well as the overall improvement within the small business sector.

f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by:

(a) victims of cybercrime; and/or

(b) insurers? If so, under what circumstances?

i. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?

No response.

g. Should Government clarify its position with respect to payment or nonpayment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

No response.

Question 3

How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?

Cynch has been fortunate enough to participate in the CCTCP program over the past year, providing us with valuable experience working to support small businesses with our regional neighbours.

One of the more significant challenges we have faced in these efforts is access to the threat intelligence necessary to align with the specific context of another jurisdiction. The threats we face in Australia are not necessarily the same as those across the region. Without understanding of these differences, any support we provide is likely to be misaligned. Australia could play a valuable role in helping collect and share such intelligence across the region.

As a technology startup, the CCTCP program provided a way to demonstrate our sovereign capability within another market. This improved access to capability across the region while also allowing us to test and enhance our solution with a new audience. The lessons we took from this were transferred back into our offering, further benefiting our Australian business customers.

The importance of small businesses to regional economies is not exclusive to Australia. For many of our neighbours, small businesses are a critical part of the fabric of local economies and present an untapped opportunity to broader reach within communities. Awareness campaigns and other programs shown to be effective in raising awareness and improving cyber security amongst small businesses in Australia could be supported across the region to great effect. The recently proposed Cyber Wardens program in development in COSBOA is one such initiative that will result in a more informed small business ecosystem that will ultimately improve outcomes across the communities they service. Cynch is excited to be developing offerings aligned to this program that will further enhance and extend these outcomes both locally and across the region.

Question 4

What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?

One major issue holding back growth in the local Australian cyber industry is access to skills. Development of pathways for learning and employment within Australian companies across the region could help alleviate this. Ideally this would be achieved via remote arrangements that would allow for local outcomes to be realised alongside support to the Australian cyber industry.

Question 5

How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?

The lack of consideration for smaller businesses in standards-setting is not uniquely an Australian issue, but one present in most nations. Embracing small businesses locally enables Australia to likewise champion for small businesses internationally. While this may not have a direct impact on the behaviour of states in cyber space, improved support for small businesses will go some way to discouraging attempts to target this key, yet vulnerable, sector.

Question 6

How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

Commonwealth Government departments and agencies should be actively championing to support local businesses, particularly those actively working to build sovereign capabilities. As it stands there is little advantage to Australian cyber security companies supplying the Commonwealth Government, in fact the procurement processes themselves favour much larger multi-nationals more likely to draw on offshore capabilities as they have been given a chance to prove themselves in other markets.

Minimum cyber security requirements in government contracts are a significant barrier for smaller businesses wanting to secure government business. Accompanying this requirement with a simple 1-pager that lists industry solutions available to help improve their cyber security, and increase the likelihood of winning government business, will provide powerful incentives to taking meaningful action.

A review of procurement practices to identify other cyber resilience barriers to small business participation could lead to process changes that break down these barriers further and encourage these businesses to address unacceptable risks.

Question 7

What can government do to improve information sharing with industry on cyber threats?

While there is a growing assortment of information sharing inside of the cyber industry, little has been done to improve the visibility of this information publicly in a way that would enable small businesses to effectively protect themselves.

Access to cyber risk and resilience related data for small businesses is patchy at best. Encouraging the capture and sharing of small business related data across government and industry would enable greater investment from solution providers and small businesses alike. Highlighting small business specific insights wherever available and exploring ways of increasing visibility into this critical area so that more informed decisions can be made would help. Regular releases of data captured through report.cyber.gov.au, similar to that published by OAIC, would be a logical place to start.

Data capture and sharing should be aligned to the desired outcomes (e.g. those defined in a Cyber Security Act), and should include the reasons why such measures are relevant to small businesses. Inclusion of case studies and real work examples in such reports will assist in making such information relatable to small businesses and increase the chances of action being tak

Question 8

During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?

No response.

Question 9

Would expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?

This could be effective but only if coupled with greater transparency and public sharing of the information collected. Increased transparency may act as a deterrent to notification however so a balance may need to be struck. Inclusion of small businesses in this notification regime may result in a significant increase in the number of reports, providing greater anonymity to all businesses in the process.

Out of options

While Cynch does not directly provide incident response services, as one of the few small business focused cyber security companies we are frequently contacted by small businesses who have exhausted all options. In every instance victims have actively notified many government entities yet received no benefit or support from doing so. While they appreciate the overall goal of reporting, few indicate they would report next time an incident occurs as they are not confident it is doing anything meaningful.

Question 10

What best practice models are available for automated threat-blocking at scale?

No response.

Question 11

Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

Cyber skills are needed in every business, not just those with a heavy STEM emphasis. While it's not necessary for everyone to be a cyber security expert, there should be someone in every business that understands cyber risks and how to manage them. This need sits alongside the need for every business to have access to digital skills, something well beyond the STEM agenda.

The recently proposed Cyber Wardens program (https://cyberwardens.com.au/) in development at COSBOA will result in a more informed small business ecosystem that will ultimately improve outcomes across the communities they service. Cynch is excited to be developing offerings aligned to this program that will further enhance and extend these outcomes both locally and across the region.

Question 12

What more can Government do to support Australia’s cyber security workforce through education, immigration, and accreditation?

To address the cyber security skills gap, programs that connect cyber security students and trainees with small businesses seeking cyber security advice and support should be explored. This would provide valuable work experience in engaging with business stakeholders as well as pathways to future employment while also providing affordable access to cyber expertise to small businesses.

IT support providers play a crucial role in the technology aspects of Australian small businesses. Cyber skills development amongst providers supporting small and medium sized organisations could be achieved through the creation of apprenticeship and traineeship programs. States have been actively investing in the tertiary education of cyber security experts, but there remains limited pathways from these courses into the workforce. By incentivising the hiring of entry level roles into businesses who can afford to support them, the size of the cyber workforce in Australia will grow.

Question 13

How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?

No response

a. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

A simple, focused place for reporting of cyber incidents would be highly beneficial to small businesses and potentially necessary in the event that they are brought into scope of legislation and regulation. It would be interesting to see this developed in such a way that reporting obligations in commercial agreements could also be simplified, potentially through an information sharing arrangement with private sector parties.

However incidents are reported, increased sharing of information and insights through this process publicly will be critical to guiding Australia’s overall cyber security improvements.

Question 14

What would an effective post-incident review and consequence management model with industry involve?

No response.

Question 15

How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?

Cyber.gov.au and other services have begun to provide direct support to small businesses responding to a cyber incident or looking for general advice. Providing more advisory based access to small businesses through such services should continue to be explored. This may help identify specific gaps, focus towards areas contextually relevant and then answer any specific or immediate concerns.

Feedback from this type of service can be used to inform and develop more scalable and automated solutions.

"Designed for a bank not for a team of 4"

Some of our most actively engaged customers have been looking for solutions to their cyber risks for years. They are motivated and ready to get their hands dirty but continually run into solutions and providers geared to helping much larger organisations. We often hear of quotes for $20,000 or more just for an assessment or solutions "*designed for a bank not for a team of 4*" where some simple changes to systems they already have in place are all that's needed.

a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

There are currently minimal incentives for small businesses to invest in cyber security beyond addressing the direct impact of an incident. As demonstrated through the success of the UK Cyber Essentials program, certification can act as a motivator for small businesses when aligned to an achievable and meaningful outcome. To account for the pitfalls of the Cyber Essentials program though, the underlying design must account for changes in the threat landscape and be actively resourced and maintained over time.

The establishment of funding grants for small businesses looking to improve their cyber resilience should be considered and aligned to baseline measurement adoption, ideally with approved solution partners willing to provide affordable solutions. Funding grants should be upfront rather than reimbursement-based to lower the barrier to adoption, but should have a requirement placed on the small business to demonstrate they have achieved the baseline cyber resilience measure within a period of time (e.g. 12 months) to ensure they remain motivated to continuously improve. The eligibility criteria for the grant should be meaningful, potentially aligned to supporting the small business to improve their compliance with procurement opportunities, therefore encouraging growth of the Australian economy, or to support capability building within their own team to sustainably manage cyber resilience over time.

There are components of the Essential 8, and other industry standards, that require significant investment, well beyond the means of most small businesses. Establishing partnerships and services with large industry partners such as Microsoft, Telstra, Splunk, Xero and banks to collaboratively support small businesses with their capability could deliver outcomes at scale. It would be important to consider the relative level of risk within small businesses and ensure that the services provided are right-sized and usable, but if established correctly this approach could provide a pathway for entry level roles into security as well.

Wrong Fit for Risk

The initial attempt by the Department of Employment and Workplace Relations to right size cyber security assurance for providers under the “Right Fit for Risk” process instead created a new barrier and unacceptable expenses for smaller providers. Cynch worked with a number of these providers in the early stages of the program, including a 2-person team, that were directed through the process to complete an ISO 27001 self-assessment, using the 700+ requirements of the ISM as an input, as well as fully adopting all Essential 8 controls. These requirements cost providers, many of whom were providing low risk services to less than 100 individuals, weeks of lost time, tens of thousands of dollars in system upgrades and immeasurable stress and anxiety as the outcome of their application and associated funding was at no point guaranteed. For some, the cost of upgrading and supporting Microsoft 365 in line with the Essential 8 was more than the cost of underpinning technology required to provide service to their handful of clients. These providers have since closed their doors.

While it is promising to see this program evolve over time to better align to provider risk, the expectations and complexity still exceeds the risk posed, especially prior to actual provider engagement.

Identifying and connecting cyber security champions across the community will empower collaboration across the economy. Reward and incentivise these individuals with public recognition or awards and provide them with a point of differentiation personally and for their associated organisations that they can leverage to continue their work. This in turn will help to increase the awareness of the broader community to the importance of building cyber resilience.

Question 16

What opportunities are available for government to enhance Australia’s cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

Government can incentivise greater support for small businesses amongst solution providers by actively promoting those with well aligned and affordable offerings. Whilst this challenges the Government’s position of not promoting any particular vendor or solution, it should be recognised that this position in itself is a barrier to success. Doing so should create opportunities to engage with other providers in ways that will enable solutions to be tailored to the local small business market.

There are ways to promote providers with appropriate solutions without directly recommending them.
Government-supported initiatives such as creating advertising/marketing grants for small business aligned solution providers, regular public mentions of success stories by ministers and public figures and including cyber solutions in the list of available vendors to small business applying for digitisation grants could all directly contribute to the adoption of these solutions and growing the interest of other vendors to support small businesses.

Question 17

How should we approach future proofing for cyber security technologies out to 2030?

The cyber risks we will be grappling with in 2030 will be different to those we know about today. This may be true even as soon as 2024.

Focusing on the principles associated with managing risk and adapting to change, as opposed to adoption of specific technologies or controls, is therefore key. Looking for ways to encourage ongoing investment into management of cyber risk, not the ticking of compliance boxes, will help Australian businesses become cyber fit, not just cyber secure against today's threats.

Key to this will be more timely information sharing and systems that take this information and translate it into actionable insights. A diverse, local cyber innovation capability that can turn these insights into solutions for every business will ultimately deliver the most cyber secure nation.

Question 18

Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?

The time and cost associated with certifications such as ISO 27k, iRAP and DISP make it next to impossible for many smaller organisations to engage with larger government departments until they have either achieved a meaningful level of commercial success or taken on a significant level of external investment. Opportunities for smaller, less established businesses to work with the government may be created by establishing guidelines that enable lower risk activities to be procured without the need for such certifications to be in place in the first instance.
Incentives (e.g. direct funding) for small suppliers to achieve desired levels of accreditation will also help address the inherent risk associated with such arrangements, while also maturing these smaller suppliers in ways that will unlock further opportunities beyond any individual contract.

A focus on minimising the inherent risk associated with an innovative supplier arrangement would be necessary to enable this approach. Agreements structured to allow value and security demonstration with upfront funding of a pilot or limited delivery scope may enable departments to more actively work with smaller suppliers.

From Small Beginnings

In 2021 Cynch, in partnership with AustCyber and the South Australian and Queensland Governments, undertook a pilot aimed at improving the security of smaller defence suppliers, The funding of this pilot enabled direct support for 50 suppliers, as well as an opportunity to build and demonstrate capabilities foundational to the Cynch Critical Infrastructure supply chain solution.

Question 19

How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

Australia has a flourishing and diverse innovation ecosystem, supported in no small part by incubators, accelerators and higher-education programs across the nation. These programs offer a focus point for the introduction of security by design as they are often working with innovators at the earliest stages of development. Incentivising inclusion of these concepts as part of these programs through funding or subsidised support would be an exciting opportunity to explore.

Question 20

How should government measure its impact in uplifting national cyber resilience?

A cyber resilient nation is one that is well informed and adaptable to attacks.

The number of attacks detected and incidents reported would be an effective means of understanding how informed we are to the threats. This information is unknown for small businesses today and a major contributor to why the sector remains immature.

Number of reports vs measure of harm caused. Reports should go up but their impact should go down.

Adaptability to attacks can be measured by the harm caused by incidents. In the small business sector this is typically understood best as financial harm however at a national level there would likely be other considerations. An alternative measure may be overall investment into cyber security, ideally tracked through government incentives.

Question 21

What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

Tracking of security budgets across sectors (e.g. government, enterprise and small business) would provide some transparency into how effective the strategy has been at incentivising prioritisation of cyber security. CISO Lens have previously shared data of this type (https://www.cisolens.com/benchmark) providing a series of benchmarks to compare to over time.

With access to skills a key constraint to growth in cyber security, the number of people employed in cyber security roles and companies locally would provide a meaningful measure.

To be considered the most cyber secure nation though, Australia will need to be able to compare itself to other nations. However this is done, it will be important to factor in the contextual factors of each nation.

Working to better capture and measure cyber context with our regional neighbours in the first instance and map these to implementation outcomes of the Strategy would be an appropriate first step.

ABOUT THE AUTHOR

Cynch Sec Pty Ltd (Cynch) is a proud Victorian-headquartered cyber security startup, established in 2018. The team's mission at Cynch is to help Australian small business owners avoid having a cyber incident becoming the worst day of their working lives. They provide SaaS and consulting solutions that support small businesses to build Cyber Fitness (a term they use instead of cyber resilience) as well as large corporations and government departments to better manage the supply chain cyber risk of their small business suppliers.

121 KING ST,
MELBOURNE
CYNCH.COM.AU

cynch