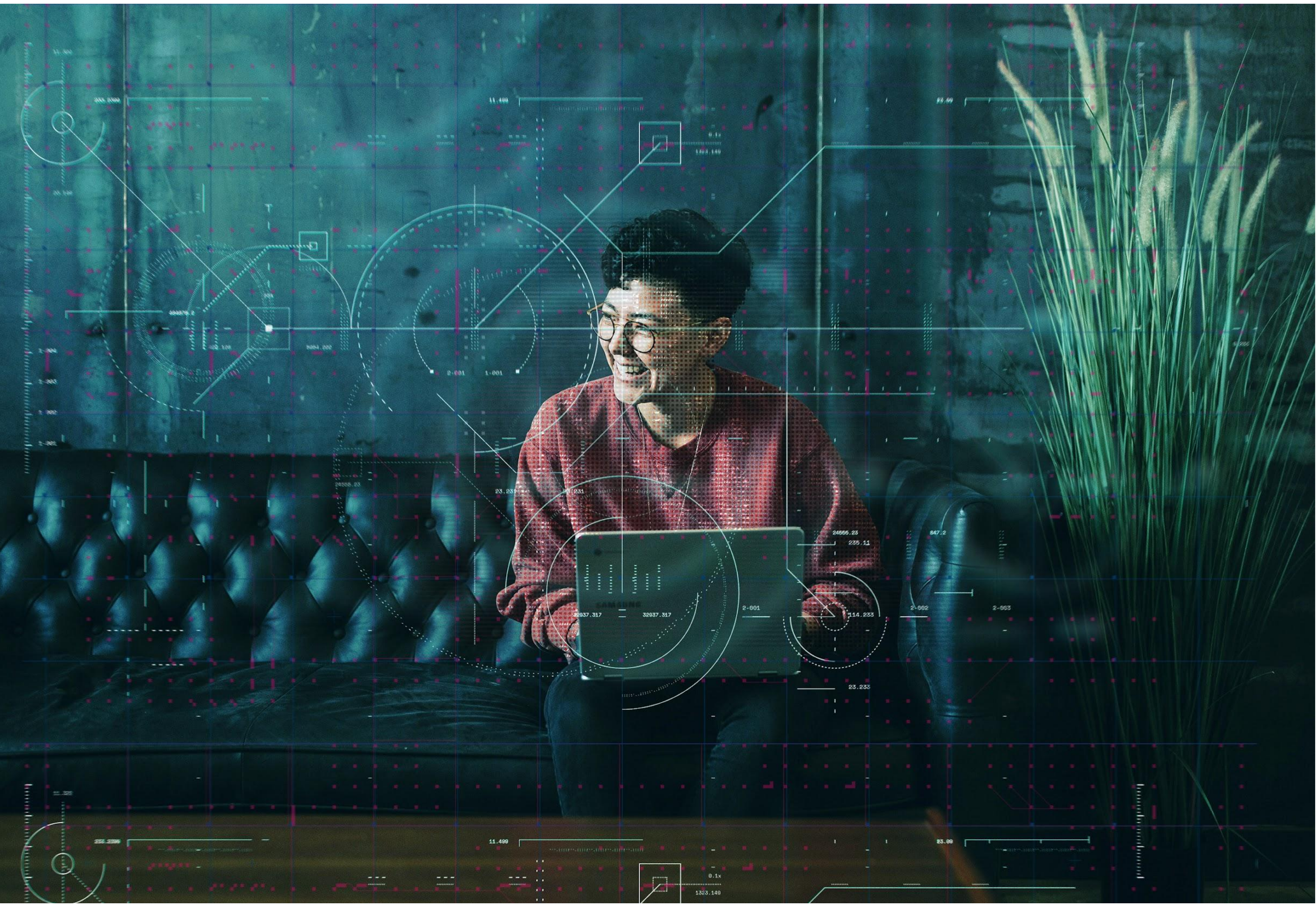
# STRENGTHENING AUSTRALIA’S CYBER SECURITY REGULATIONS AND INCENTIVES

## Cyber Fitness for Small Business

## Submission by Cynch Security

August 2021



# INTRODUCTION

Hi there!

At Cynch Security, we live and breathe small business. Our business has always worked with the mission of creating a world where every business, no matter their size, can be fit and strong and resilient to the cyber threats faced today. To realise this vision, we support typically under served smaller organisations build cyber fitness.
In responding to the call for views to the Strengthening Australia's cyber security regulations and incentives, we have focused our comments towards the following areas where we have direct experience and expertise:

- Small businesses and how they experience cyber incidents and utilise cybersecurity products and services;
- How people at the heart of every organisation are affected by the decisions ultimately made by the Government and industry; and
- Challenges surrounding smaller suppliers as they navigate the security obligations associated with supporting government departments and large enterprises.

Based on the above, we have not made comments in response to every question posed in the call for views, however we trust those comments we have provided are of value.

We hope this document assists in strengthening Australia's cyber fitness, and we look forward to supporting related efforts in the years ahead.

Sincerely,

Adam Selwood
Co-Founder & CTO
Cynch Security

Our mission is to build a world where every business, big or small, is fit and strong and resilient to the cybersecurity threats we all face every day.

## 1. What are the factors preventing the adoption of cyber security best practice in Australia?

Businesses know that solving cyber security issues can involve something broader than just technology. Yet they remain unclear about what they need for their business to be cyber secure in the ever-changing cyber security landscape. While there is a wealth of resources out there, figuring out what is relevant and achievable in a specific business context is next to impossible without the support of an expert or expensive tooling.

Affordable and effective solutions from providers such as Cynch Security are emerging, but small businesses often find it difficult to determine who to trust. Those businesses that successfully navigate through the complexities of the cyber security market will act, but only if they are motivated to make it that far.

A clear theme that emerged through a study undertaken by Cynch Security, Deakin University and RMIT in 2020[1] is a desire for targeted recommendations that speak to their specific circumstances. A key complaint about cyber.gov.au is that the information is too general, making it hard for business owners to apply to their own circumstances. Checklists and case studies focused on industry and business size were suggested as one way to address this problem. Small businesses don’t expect personalised support from free sources like cyber.gov.au, but the generic approach is not working.

The study also found that two out of five small businesses have direct experience with a cyber incident worthy of reporting at some level. Even with so many incidents occurring, these stories are rarely shared publicly. It is likely, most would prefer to simply deal with the issue as quickly as possible and get back to business. Without an incentive to share, small business cyber incidents are likely to remain behind closed doors and obscure the fact that it really could happen to anyone.

Without increasing the visibility of cyber incidents amongst small businesses and improving the relevancy of guidance, small businesses will more likely than not wait to adopt best practice, or take any meaningful steps, until it is too late.

## 2. Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?

There needs to be a significant cultural shift amongst Australian small businesses. This will either happen organically as more feel the pain directly, or proactively through concerted efforts on part of industry and government. No single area is responsible, we all need to work together.

[1] https://cynch.com.au/small-business-cyber-fitness-2021

Collaborating as an ecosystem is a challenge in and of itself. While ACSC's central role in supporting cyber security across Australia is now established, the focus towards defensive aspects in the context of the small business sector limits the reach of their messaging. Many small businesses are more aspirational in their investment of time and finances, and while cyber fitness can act as an economic growth enabler, there is little mandate or expectation that ACSC would talk to those benefits. Other departments may be better positioned to champion for stronger cyber fitness amongst small businesses, however to date this doesn't appear to be an area of focus.

## 3. What are the strengths and limitations of Australia's current regulatory framework for cyber security?

While we are always on the lookout for meaningful examples to share with small businesses, there are few obvious case studies that would motivate a business to take action. While small businesses are often excluded from regulation in this area, there are few public examples to draw from of any size that can demonstrate the consequences of inaction or acting inappropriately.

Without real consequences and public examples, regulation will remain easily dismissed and ignored in favour of other material risks.

## 4. How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?

The Privacy Act is a good basis to work from, as most businesses are aware of it already in some manner. Extending the obligations to smaller businesses, as a minimum to those with employees, would provide a clear starting point for many to anchor to as it has already amongst larger organisations.

There should also be addendums to the act regarding security obligations, though they should align to a shared understanding of responsibility to ensure multiple parties, that could rightly be considered victims of an attack, are appropriately protected.

## 5. What is the best approach to strengthening corporate governance of cyber security risk? Why?

The CISO Lens Benchmark report[2] includes insights on the approach to security investments and other challenges within large Australian organisations. These insights help to inform discussions amongst businesses of all sizes as they provide a place for scoping and investment to aspire or align to.

[2] https://www.cisolens.com/benchmark

We would love to see large organisations increasing transparency in their approach to cyber risk and believe such data would greatly benefit the broader ecosystem by setting a strong example for small businesses. Continuing to keep such insights to boardrooms and internal stakeholders will leave the rest of Australia in the dark as to what is or isn't working.

## 6. What cyber security support, if any, should be provided to directors of small and medium companies?

Directors of small and medium companies are just as deserving, if not more so, of cyber security support as any other. To ignore them, as is what has historically been the case, undermines the entire Australian economy.

Large companies, government departments and other organisations don't operate on an island. Each of them rely on, in some way or another, smaller organisations. Traditional supply chain risk approaches will 'tier out' smaller suppliers as they are considered low risk, leaving most exposed and vulnerable to an attack that could have a massive impact across a number of organisations.

For those fortunate enough to be deemed 'worthy' of having their cyber security assessed, most will be asked which massively expensive and complicated certifications they have, as well as dozens, if not hundreds of other complex, often irrelevant questions. Many small businesses don't make it past this point, greatly reducing the viability of many and limiting innovation and growth across the economy. We can support small businesses looking to work with larger organisations by approaching supplier assurance as a partnership, instead of an adversarial activity. Providing smaller suppliers with an achievable set of requirements from day one and then supporting them as they mature to a more tolerable level would ultimately benefit all parties.

Helping smaller businesses understand and take meaningful steps to address their cyber risk is the least we can do to support this desperately under-resourced but fundamental sector of our economy.

## 8. Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?

While there is an overlap in privacy and security concepts, there is significant enough importance and uniqueness for a stand alone cyber security code to exist.

Adding a cyber security code under the Privacy Act would make sense if the intent is to protect information, but may detract from the purpose and value of the Privacy Act itself and reduce focus on broader aspects of cyber security. More complexity to the Privacy Act would likely create more confusion around the standards and requirements.

It may be better to establish a separate code with linkages back to the Privacy Act as well as other industry standards such as the ACSC ISM, ISO 27000, NIST and others.

## 9. What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?

Mandating Multi-factor Authentication inline with the example set by the ATO as part of the push to cloud accounting platforms would be a sensible first step. Recent changes within the ACSC's Essential Eight maturity model provide a strong basis for this control.

While other items within the Essential Eight may be achievable, their cost effectiveness for smaller businesses can be a challenge. Those measures achievable within commodity, though modern, technologies should be considered a mechanism for encouraging businesses to maintain their technological environment. Examples of these controls include:

- Installing applications from trusted sources only
- Hardening web browsers
- Enabling automatic updates
- Limiting administrator access

While the question requests technical controls, policy and behavioural controls should not be neglected. Assigning responsibility for cyber risk within an organisation, similar to the role of a privacy officer, should also be considered alongside regular training of staff to ensure a culture of cyber fitness is endorsed beyond the boardroom.

## 10. What technologies, sectors or types of data should be covered by a code under the Privacy Act to achieve the best cyber security outcomes?

As a minimum, all externally facing technologies and data should be covered, potentially also including anything accessible from an external connection.

Guidance on how to identify and classify other technologies and data based on sensitivity or criticality should be provided to guide other considerations.

We strongly recommend all industries and sectors of the economy be included in order to remove ambiguity and reinforce the importance of cyber security across Australia.

## 22. Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?

While responsible disclosure programs are typically the realm of larger businesses, we would welcome further exploration into how a similar approach could be implemented for smaller businesses. A central triage service operating on behalf of smaller organisations that could then assist in addressing issues as they are reported could be highly valuable within Australia. Such a service, once established, could provide a mechanism for direct notification to organisations when large scale attacks are observed by the likes of ACSC.

With or without such a service there are developments within the ecosystem that will push in this direction regardless, leaving small businesses exposed and at risk.

## 23. Would a cyber security health check program improve Australia's cyber security? If not, what other approach could be taken to improve supply chain management for small businesses?

Every small business will at some point want to understand their cyber risk, however few will have significant resources they can deploy to find the right answers. A cyber security health check program can provide some important insights to many, but should really only be seen as a first step on a much longer journey towards cyber fitness.

The Cynch Cyber Fitness platform was developed with this in mind, having provided health checks and guidance to over 500 Australian businesses to date, including many across various supply chains. Key to any improvement in the small business sector is identifying cyber fitness champions within teams and then supporting them through achievable, approachable and relevant guidance.

Cynch has worked with a number of larger organisations on small business supply chain management in recent years. Approaching the problem as an opportunity to strengthen relationships, instead of challenging a relationship as is traditional, is critical.

While the outcome of a health check or assessment is an important first step, without additional support it will often get put on a shelf until spare resources materialise. Giving small businesses access to appropriate support first, and then using a health check or assessment to inform that support, yields better security and business outcomes.

## 24. Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?

Publically recognising businesses that have adopted or are aligned to best practice could provide a commercial point of differentiation in some instances. This may however be limited to industries or geographies where it is harder to differentiate. Consumer sentiment would need to shift for this to become a strong motivator amongst large numbers of small businesses.

Our research found more than half of small businesses are comfortable that they are meeting customers' expectations already[3], suggesting little motivation to do more to secure their business is coming from consumers. In practice we have seen more motivation coming from smaller businesses pressed to take action by larger organisations through supplier assurance activities. Unfortunately, these tend to focus on more extensive and challenging certifications such as ISO 27001, posing a significant burden on already constrained small businesses. A more appropriate and achievable alternative for small businesses would be well received in these contexts, provided it was respected amongst larger government and non-government clients.

Combining a health check program with incentives such as grants, greater access to government contracts, or discounted access to other resources can also be an effective motivator. Private sector partnerships with small business suppliers such as business banks, insurers and technology vendors would be worth exploring in this context.

## 25. Is there anything else we should consider in the design of a health check program?

Any health assessment must consider the context of the organisation. If the check focuses on technologies or areas of risk that are irrelevant to a business, the results will similarly be meaningless.

Likewise the health check should be meaningful to small business customers. As consumers, we all recognise and respect the Australian Made and Energy Rating schemes as carrying value. Without similar understanding amongst consumers, businesses may see little value in pursuing a similar security recognition. Marketing the program broadly should therefore be considered.

While the UK Cyber Essentials program is a fantastic reference point, since it was implemented the technology and threat landscape has shifted, reducing its usefulness over time. Many of the requirements (similar to the Essential Eight) assume a business operates from an office and hosts many of their systems themselves. Most (if not all) small businesses now primarily operate on cloud systems

[3] https://cynch.com.au/small-business-cyber-fitness-2021

and often remotely. Similar changes should be expected in years to come, and the health check designed to evolve accordingly.

There is also a wide array of cyber security standards businesses could align to. Where possible, look to align the health check to existing standards and requirements. This can help optimise the path for small businesses as they grow and open opportunities for them to adopt more mature, international standards in the future.

## 28. What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights of consumers?

The ATO has been highly effective in introducing MFA amongst the cloud accounting space. Where possible, similar mandates or policies from the government should be considered to influence control adoption across large aspects of the business ecosystem.

Balance needs to be struck regarding policy decisions where small businesses are involved. Continuing to exclude small businesses, in line with the Privacy Act, will leave them vulnerable and unsure of what they should be doing. Similarly, asking smaller businesses to follow the same rules as larger organisations will disadvantage and lock them out of opportunities. Look to establish a middle ground between all or nothing, ideally with some element of support to help small businesses along the way.

Finally, where minimum standards or requirements are established, look for ways to ensure they can be adopted without any additional costs to small businesses or consumers. Asking smaller companies and individuals to pay for security that is considered a minimum pushes the burden onto those most at risk and least able to pay. We aren’t charged for seat belts when we buy a car, similarly we shouldn’t need to pay to protect our accounts with more than a password.

Cynch is an Australian based company on a mission to ensure every business, big or small, is fit and strong and resilient to the threats we face every day. We partner with business owners, continuously profiling their cyber risks and providing them with everything they need to build their cyber fitness.