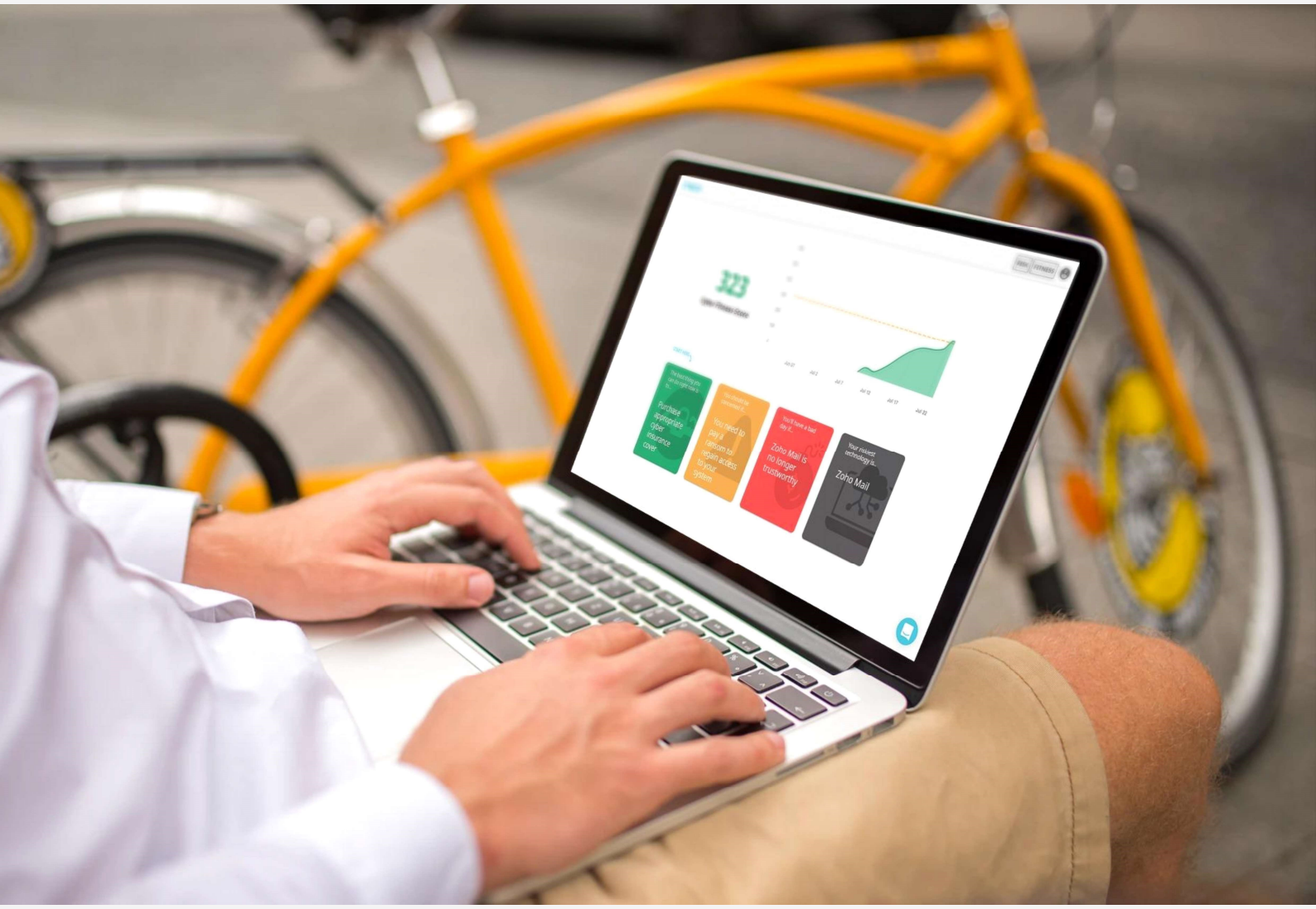
CYNCH

CYBER FITNESS FOR SMALL BUSINESS

Australia's 2020 Cyber Security Strategy

Submission by Cynch Security

October 2019



INTRODUCTION

Hi there!

At Cynch Security, we live and breathe small business. Our startup 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 businesses with fewer than 50 staff to become cyber fit.

In responding to the call for submission to Australia's 2020 Cyber Security Strategy, we have focused our suggestions around the following areas where we have direct experience and expertise:

- Starting and growing a cybersecurity startup in Australia that has global applicability and ambitions;
- Small businesses and how they experience cyber incidents and utilise cyber security products and services; and
- How people at the heart of every organisation are effected by the decisions ultimately made by the Government and industry;

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

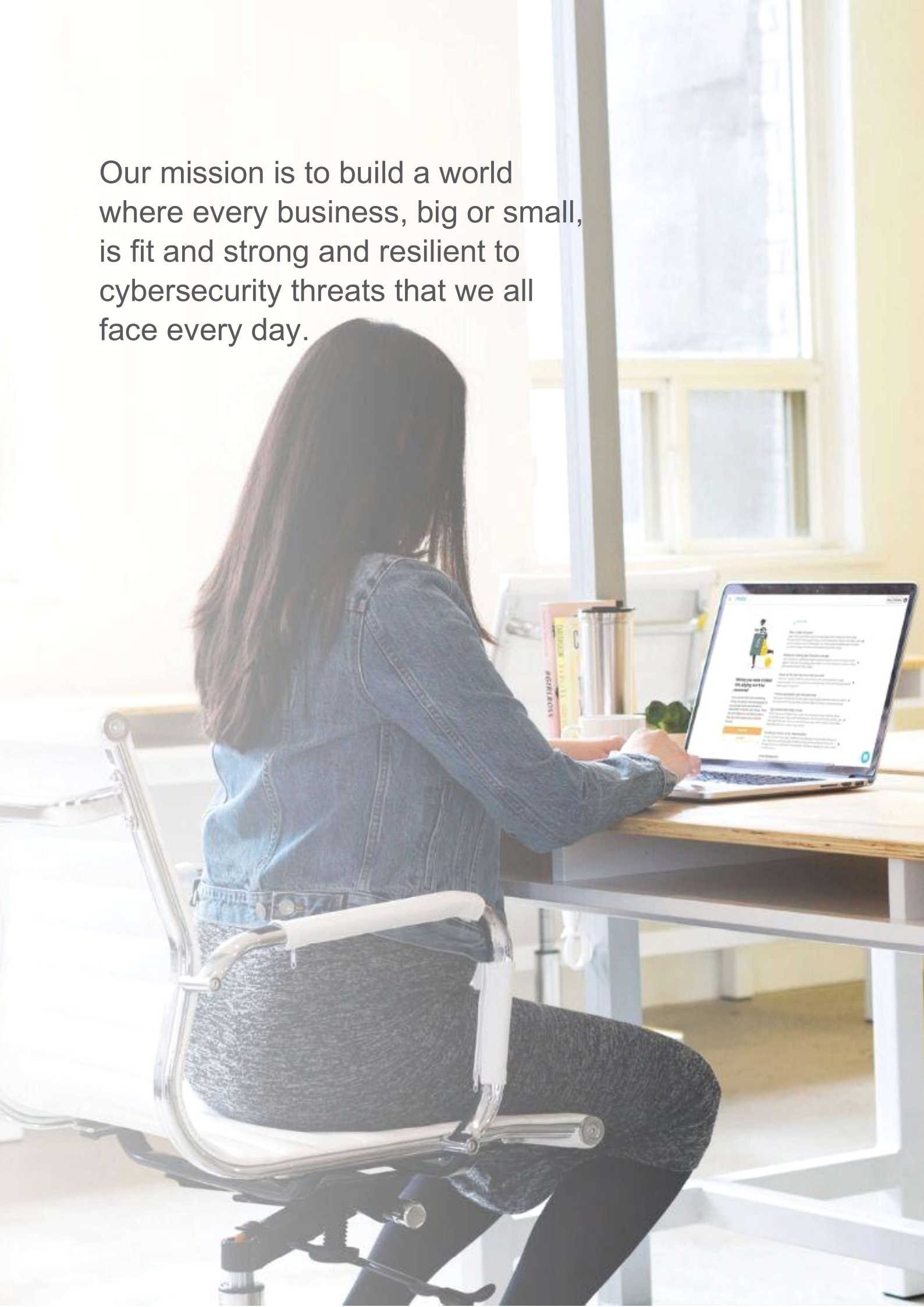
We hope this document assists in the creation of the 2020 Strategy, and we look forward to reading it and acting upon the recommendations in due course.

Sincerely,

Susie Jones
Co-Founder & CEO
Cynch Security

Table of Contents

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



WHERE ARE WE NOW

What is your view of the cyber threat environment? What threats should Government be focusing on?

The Managed Service Provider Partner Program (MSP3) was designed to uplift the cyber security posture of MSPs in Australia, and was developed in response to the global compromise of MSPs as part of the Cloud Hopper operation.

Whilst we fully support this program, we observe that micro and small businesses (those typically with fewer than 50 staff) are particularly exposed to these same threats targeting MSPs, but there is no corresponding program to assist them. Many businesses of this size do not have ongoing service agreements with MSPs, and so will not benefit from this program even indirectly. Business Email Compromise, for example, is a growing problem for this market and they could use government support to address this.

Furthermore, we believe there would be significant benefit to small businesses in high-risk supply chains (e.g. Defence) if Government directed additional resources towards threats to these industries. As small businesses are more likely to fall victim to attacks whilst simultaneously being less prepared to respond, the value that Government could provide to those in high-risk supply chains would be greater than in other industries.

We are building a brand and culture in Cynch with business owners, not technologists, at its heart.

POSITIONING OURSELVES FOR THE FUTURE

Government's role in a changing world

What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?

We believe all levels of government should continue to work to raise awareness of cyber threats across Australia. Government should also continue to play a role in helping at-risk communities and organisations, including (but not limited to) micro and small businesses, understand the resources available to address their risks. Publicly providing advice on how these groups should respond when new threats emerge, in plain language, will help strengthen our society from the ground up.

Furthermore, providing small business guidance for security guidelines such as Essential 8 (which is virtually impossible for a small business owner to interpret and apply in its current form) will have a positive effect on the security posture of small business owners without in-house technical skills.

Providing incentives to those working in adjacent vocations and industries to encourage them to develop cyber skills will help broaden the reach of cyber security messaging, reduce the impact of select cyber skills shortages, and speed up improvements across the country overall.

Finally, there may be a role for Government to play in providing insights across the entire ecosystem when they are born from the most commonly used technologies being targeted by new threats (e.g. aggregated risk situations).

Enterprise, innovation and cyber security

What role can Government and industry play in supporting the cyber security of consumers?

Increasing awareness of how consumers can identify and work with micro and small businesses safely, for example teaching them questions to ask their local accountant about how their information is stored and transmitted as well as providing guidance on what a good answer might sound like. By doing this, consumers can educate themselves on the risks and improve their security, and small businesses will be motivated to meet the growing expectations of their customers and clients.

How can Government and industry sensibly increase security, quality and effectiveness of cyber security and digital offerings?

Government accreditation of secure products and services (eg Cloud service providers) provides a huge incentive for tech companies to invest in improving the security of their products and services. It also provides those procuring services with assurance that they have secure options to choose from. Existing accreditation programs (i.e. IRAP) can be quite onerous and at times inappropriate for many digital solutions. Establishing a less onerous accreditation program for lower risk digital offerings would provide a stronger initial foundation for providers to align to.

Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effects be?

The MSP3 program and new similar programs for other sectors (such as one for small businesses) could be outsourced to the private sector by the Government granting the ability to certify compliant businesses to private organisations (such as industry bodies) who can then offer accreditation when criteria has been met. The UK Cyber Essentials program is a great model to look to for how this is done well.

What specific market incentives or regulatory changes should Government consider?

The Notifiable Data Breach Scheme (NDB) has not had the effect on Australian citizens and companies as similar laws overseas such at GDPR, and we believe this can be largely attributed to the relative weakness of the laws and penalties in comparison to overseas equivalents, as well as a lack of visible enforcement of the potential penalties by the responsible authorities. A law is not effective if it is viewed as unenforceable or insignificant when enforced, and we feel this should be addressed with haste. Furthermore, extending the NDB to all businesses operating in Australia will help incentivise small businesses to start improving consumer protections.

Expanding APRA's CPS-234 to (eventually all) other industries, and then enforcing audits against these requirements, would quickly move the needle in terms of investment by public and private companies into security, as well as improvements in their overall security posture.

On a different note, currently there are no incentives for local organisations to buy from Australian companies. Various countries around the world have direct incentives in place to encourage buying locally, and yet our economy in many ways does the opposite. Providing monetary incentives such as tax breaks to purchasers could be funded by taxes paid by those selling the local products and services, whilst stimulating job and economic growth across Australia.

Whilst growing a local cyber startup in Australia is very hard, just getting the capital together to start one is even harder. The original HECS (and now HELP) scheme was established to improve access to tertiary education for Australians and has resulted in significant increases in the number of students successfully completing tertiary studies. A similar program established to offer low-interest and low-entry loans for promising startups in industries targeted for growth would ease the number of startups that fail due to slow initial revenue growth. This would also encourage more experienced people currently working in large corporates to take the giant leap into starting their own enterprise.

Another attraction to joining the burgeoning local startup economy has been the AusTrade missions that have been undertaken have been widely lauded as a success. Plans by AusTrade to no longer organise and lead these missions leave a significant gap in our ability as a nation to show our skills to the world. If they don't run them, who will? No-one else is funded or better positioned to do so. Australia will quickly be forgotten in a busy global cyber market if we are not visible and introduced to the global community.

Adjacent Government run programs can also assist with cyber security. A key driver behind small business adopting good cybersecurity practices is the level of digital adoption in their business. The more reliant they are on technology, the more efficient their business, but also more aware they are of their risks. Programs such as the Federal Government's Small Business Digital Champions program serves as a fantastic example of government helping small businesses to adopt new tech in order to grow their business. Cynch is a corporate partner in this program, and we are helping these businesses to improve cybersecurity alongside this adoption, and the expansion of this program will serve this market extremely well.

Lastly, we should look to our overseas counterparts. The UK Cyber Essentials program has been incredibly successful for the UK, and adoption and support of a similar program here in Australia could see us experience the same drastic improvement as they have there.

A trusted marketplace with skilled professionals

How could we approach instilling better trust in ICT supply chains?

Certification programs such as the UK Cyber Essentials accreditation program are great for assisting with this risk, as well as auditing and enforcing current regulations such as CPS-234 that require supply chains to be appropriately managed.

Are there barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?

The Australian cyber insurance market suffers from a lot of misinformation surrounding the value and use of the product. Insurance brokers in the main do not understand cyber risks, and therefore cannot sell the benefits of the policy as a viable risk transfer option to their clients. Insurers in the main do not make their insights from claims available to the public, so the claims being paid are not visible. Many cybersecurity professionals do to understand the elements of the policies and so incorrectly criticise the policies and their adoption as being replacements for protective measures, rather than support for response to (and recovery from) incidents. Cyber insurance is also largely only available to businesses, with few (if any) effective policies being designed for and made available to consumers.

By improving education on the intent and coverage of policies and the risk elements they mitigate, expanding coverage to consumers as well as corporates, and sharing data both with and from insurers, this market could rapidly grow and serve the entire economy.

How can high-volume, low-sophistication malicious activity targeting Australia be reduced?

The Cyber Security Small Business Program that was recently closed was developed to support small businesses with fewer than 20 employees across Australia to have their cyber security tested by a provider that has been approved by the Council of Registered Ethical Security Testers Australia New Zealand (CREST). Unfortunately, providing a small business owner with the results of a health check or a penetration test only adds to the confusion if it doesn't come with plain language advice on what can be done with the results.

Expanding this initiative to other services that provide risk advice, prioritisation and solutions would expand the reach of the program, and the effectiveness overall. Furthermore, by expanding the number of businesses who are accredited to deliver such services will assist to meet the demand from small businesses. Finally, increasing visibility of high-volume, malicious activities targeting Australians will assist those actively involved with threats prioritisation. A publicly consumable source for data surrounding high-volume, low-sophistication attacks would also assist in making these types of threats real for smaller organisations that currently have no visibility of the situation.

A cyber-aware community

To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?

We believe that a lack of cyber awareness contributes to poor choices being offered and made by consumers, but this is not the entire issue. Poor communication via our fractured market is a significant factor. A significant amount of the advice provided on how to act is too general and not contextualised for the users, so people can't see the relevancy to their own lives.

For example, telling a small business owner "to enable multi-factor-authentication on all critical systems" will likely be ignored, but saying "enabling multi-factor authentication in your email system will mean that even if someone discovers your password your emails will stay safe. Let's show you how to do this ..." adds specific context that makes less abstract and more relevant. This added relevance helps motivate an individual business owner to act.

The Government teams behind the content developed and published on cyber.gov.au are often under-resourced, and yet have largely not collaborated externally. By doing so they could improve the effectiveness of the content, the language used, and the adoption of this advice greatly. By keeping it entirely in-house, you are potentially limiting the channels available to get the messages out there.

How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?

Greater consumer focus will incentivise businesses of all sizes to invest in cyber security. This will increase investment in the cyber security market globally, and if Australian businesses lead the way they have the chance to capture a greater slice of this bigger pie. Products that enhance the visibility of security amongst consumers (e.g. cyber fitness score) will benefit greatly and help consumers to make better choices.

Would you like to see cyber security features prioritised in products and services?

Products that provide externally auditable insights regarding the cyber security of the technology would be beneficial in raising awareness and motivating businesses to make better security decisions.

Other Issues

Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?

Small businesses need help, they need assistance that takes into account their unique traits. Whilst it is commonly understood that small businesses have less access to technology and cybersecurity expertise, it is often not recognised that working with small businesses is significantly easier and more rewarding than working with larger organisations. Small businesses are quicker to make decisions and implement appropriate solutions and personally value the rewards of a job well done. With the right support the small business cybersecurity landscape can be rapidly improved.

We strongly encourage the Government to consider micro and small businesses in every aspect of the 2020 Cyber Security Strategy for Australia to ensure the improvements are made across our entire nation.

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.