Submission for

Australia's 2020 Cyber Security Strategy

Contents

Executive Summary

Portal Technology is a long running and established Northern Territory ICT managed services provider.

We have done great work in supporting small to medium enterprise and non-for-profits with cloud migrations and digital modernization. Regularly patching and maintaining our customer environment as well.

We have attempted to answer 9 questions that we feel as an MSP we could offer some perspective for your consideration.

We would like to thank you for this opportunity, as well as to the team from Home Affairs that came to visit Darwin for public consultation.

If you would like to speak with us further on any of our views, please feel free to reach us on

info@portaltechnology.com.au

Q7. What role can Government and industry play in supporting the cyber security of consumers?

We commend the government for the actions undertaken since the launch of the initial cyber security strategy. Government should continue this, and we suggest that government keep a focus on ensuring an even and level playing field for new and established providers of security services. Despite how initiatives to codify excellence in cyber security have proven effective (such as CREST) there is a undefined gap between newer entrants being able to catch up and win government work. From an MSP perspective, it makes it even more ambiguous when trying to support clientele that have extra government security requirements. Note that more work needs to be done to define easier pathways for growing cyber security services firms and MSPs that offer essential security services.

Government may further assist in the development of cybersecurity for consumers by ensuring that the 'everyday' technologies and activities people undertake in, such as grocery shopping, banking, tap and go, managing their government entitlements remain operational with high uptimes. Although much of this is the duty of private industry and essential services that form the economy, government should ensure that there is enough support to assist these entities in their activities. This we understand is what currently happens and should continue to be the case.

However, with such emphasis on the larger players helping to keep Australia feeling cyber safe and sound, with business as usual, it does become a potential concern that individuals may not quite feel safe online. Much of what we have observed in the MSP space is the reporting of cyber incidents of a personal nature through a business channel for advisory. We would like to see government offer more support for firms that are in a position to assist the everyday Australian in their cyber security. There are local initiatives here in Darwin such as that by the Australian Small Business Advisory Services Digital Solutions that attempt to reach out to smaller business not in a capacity to sustain a managed services contract.

With this in mind, it would make sense for government to ensure that the conditionals were beneficial for small businesses to be able to assist in this space. Moreover, in the event that individuals do experience a cyber security incident, that they are able to be directed to a source of information and type of support to be able to help themselves.

Q11. What specific market incentives or regulatory changes should Government consider?

It would be advantageous for wider industry if government could incentivise MSP to extend their offering into managed security services. MSP's are ideally placed to succeed in this area as they are equipped with service and technical personnel. Furthermore, they provide the initial environment for which business is conducted – in a technological sense. We would further encourage the government to make the necessarily regulatory changes with matching incentives to ensure that cyber security firms are able to have themselves are able to receive security support in an assurance sense. This could be as simple as encouraging industry bodies to acknowledge a firms competency to having support from the ACSC or academia to help improve the underbelly of the nation's ICT which is what MSPs do as daily business.

Q12. What needs to be done so that cyber security is 'built in' to digital goods and services?

As a managed service provider we do our best to ensure that this is exactly what we do for each one of our clients. Although this is not the case for many businesses in different industries, those businesses that choose to engage with an ethical and responsible MSP will be better placed to succeed in this space. There is to a large degree for merchants built in cybersecurity for payments and transactions – but this does not always extend to digital goods and services.

We can imagine for Australian retailers that provide digital goods and services that they would require some assistance from the government to ensure that their products are secure. At the very least in the sense that it would become more difficult to counterfeit or to steal the intellectual property. This would tend to be taken care of by the digital partner that is assisting the develop of the digital product or service. Perhaps it would be beneficial to extend the scope of particular government programs and incentives to help in this space. From an MSP perspective we do our best to ensure that they have secure systems on which they can undertake development and run their enterprise with.

Q.13 How could we approach instilling better trust in ICT supply chains?

Our approach to ensuring trust in ICT supply chains is to use reputable vendor partners. However, this approach will often lead to only a select view distributor to be trusted thus quelling the overall market diversity. In our experience, we tend to deal not only with distributors of technology goods, but also directly with vendors. As we are both an MSP and by extension a reseller for vendors and distributors, instilling better trust comes down to vetting each part of the overall supply chain. Perhaps a larger, cyber diplomatic effort would be best to create a memorandum of understanding at the transnational level to ensure that vendor goods and services being imported will meet a benchmark market requirement first so as to alleviate the pressure on the amount of proofing MSP's must conduct. We operate as if this is taken for granted by default however it may not necessarily be the case.

Q.14 How can Australian governments and private entities build a market of high quality cyber security professionals in Australia?

As we are in the managed service industry, we are more acutely aware of the need for a larger market of high quality cyber security professionals. As it stands there are numerous ways by which talented people can develop their cyber security skill sets and be recognised as professionals. From our perspective, the type of contracts we would like to service, a key player in this space is CREST. That said however, the Australian approach to CREST is not as mature as the international approach.

There is a great deal of international professionalisms that tend to overrule or be more valued in Australia. Growing the Australian market for professionals requires a holistic approach – but not an entirely centralised approach either. The diversity is what makes this market dynamic. However, the diversity and requirement for professionals in this space also makes it difficult for aspiring professionals to develop their careers – often needing to fulfil multiple job functions rather than being able to grow and specialise.

Q18. How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?

As a managed service provider here in the Darwin region our approach to this is to always supply, configure and manage the best equipment we can source that works for our client's requirements. This is a security activity that forms part of the very basis of managed service offerings in the ICT space. The challenge in this space comes from the sheer diversity of the types of clients, their business needs, their risk appetites and finally the equipment which they use. It is not uncommon to inherit an information system with an absence of security and enterprise architecture documentation. Part of the journey from an MSP perspective to help continue to grow, mature and protect these diverse systems.

The issue with this is that as there is so much diversity, the process of proactively identifying and remediating cyber risks becomes troublesome at scale. Not only would this mean that our business would need support to develop the commercial aspect of this offering, but we would further require support to make this completely centralised. This is no small feat. As such, much monitoring not only by ourselves, but other MSP's in our region is done on a singular ad-hoc basis. We are in the process of remediating this; however it is a slow process.

Q21. What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?

From our perspective the information sharing has been quite good. Baring in mind that we are located in Darwin, Northern Territory. We feel the level of engagement despite the absence of a cyber security centre here has been good. On a local government level, we commend the NT Government for their active support of the industry. However, I cannot say that we regularly reference government material on cyber threats and vulnerabilities. Our primary source of information tends to come from vendors and cyber security industry leaders. We then fact check this against the official word from the Australian government. In the event that there is no publicly available information from the Australian government, we will cross check this with information provided by allied governments.

As a local managed service provider, we have utilised federal and local government sponsored events to make sure that we can continue to share the knowledge that we have in the security space. We have had well received results in the local business community with this. Therefore, despite how there may be constraints which we have identified and others that you would be aware of, there is activity taking place here in Darwin which should continue to be fostered and developed to assist.

Q26. Would you like to see cyber security features prioritised in products and services?

As a managed service provider cyber security has always been a priority in our product and service offering. As tends to be the case with technology goods and services, security features come in varying capacities. With this in mind we make sure to assemble the optimum suite of products and services to match not only the risk appetite of the client, but what is also economical for them too.

A greater emphasis on cyber security features is naturally taking place from what we have observed from our supply chain. Vendors and technology partners that we resell and configure to clients are emphasising, for want of a better term, the security value chain. Security aspects such as secure and verified drivers, trusted component sourcing, and vendor specific software and product support are becoming more prominent.

For ordinary consumers there would be some benefit to emphasising that a device is secure in some capacity. We find this no different to ordinary advertising to drive sales if it is a concern of the potential customer. However, it is important to consider how despite a security feature may be offered, it does not necessarily translate into real world security. Consider mobile devices that have disk encryption, a rudimentary MDM offered by the manufacturer and many options to further protect your phone and data.

Even with these offerings the average consumer may not utilise the optimum configuration; this does not even factor in the wider digital ecosystems and numerous attack vectors. From our perspective, we commend the secure MSP program run by ACSC/ASD for which we missed out on the first round of joining the program. These offerings help to signal cyber security features in products and services.

Notes from the Darwin public consultation

- Local MSPs need support to bolster their cyber security offerings to clients that might not be in a financial position to afford additional hours of service
- Local businesses in the Darwin region would benefit from having a general threat level or monitoring of recent events which is publicly available so as to gauge the security situation and risk levels of localised cyber crime
- There should be great guidelines and uniformity for the security requirements of banks and general everyday services. It gets rather confusing what businesses should do.
- Is the cyber security situation getting worse or is there a bias in effect because there is greater monitoring of it today? Is there unnecessary fear and concern?
- When individuals and small businesses report cyber crime their “customer journey” is not a good one.
- Is there enough consideration for cyber security awareness and support for peoples of disadvantaged or minority backgrounds?
- How can everyday people easily identify cyber security professionals and people and business of trust?