

How MSPs Can Prepare Their Cyber Security and Business for 2021.



Congratulations on making it through 2020.

As we know, not every business did. However, whilst the dust is certainly settling, we are still crawling through the worst recession since WW2. In these tough times, batten down the hatches and securing and optimising your business is more important than ever. That's why we've created the ultimate guide for doing so. From security awareness training to demonstrating your value, we've outlined the pointers your MSP should heed if they're to be in a good place this time next year. To start things off, let's take stock of the current cyber security landscape in Australia and New Zealand.

The last couple of years have been a feast for cyber criminals

As outlined by Accenture's third State of Cyber Resilience Research report 2020, only 43% of Australian businesses had an active, functioning cyber security policy. This has led to 55% of attacks breaching security measures. Not surprisingly, the financial losses reflect that.

Cyber security incidents cost Australian businesses an estimated **\$29 billion every year.**

Business email compromise scams is the most costly to Australian businesses, hitting **\$132 million.**

Source: Australia's 2020 Cyber Security Strategy, Industry Advisory Panel Report, July 2020
ACCC's Targeting scams report, June 2020

Then in 2020, COVID-19 was added to the fire. This caused the biggest shift to remote working in human history. With more remote work comes less security; employee-owned devices and home WiFi are easier targets for cyber criminals. Unsurprisingly this perfect storm led to a rise in phishing scams by 190%* in May 2020.

*Source: Australian Competition and Consumer Commission (ACCC)

Small Businesses were as much of a target as enterprises

According to the ACCC's Targeting Scams report:

"Scam reports from businesses were mostly from small (5-19 staff) or micro (0-4 staff) businesses, although many didn't report the business size. Medium (20-199 staff) businesses reported the highest losses, but micro businesses experienced the largest number of scams resulting in a financial loss."

Regardless of size, businesses will be affected at some point in time and as Service Providers need to ensure we are supporting them with multi-layered defence.

If that comes as a surprise, consider the following. According to the ACSC Small Business Survey, one in five small businesses that use Windows, have an operating system that stopped receiving security updates in January 2020.

Cyber criminals will find opportunities with all sizes of business. In a survey of 1007 Australian employees¹, 43% of all cybercrime targets were on small businesses. The Australian government states that 98% of all Australian businesses are SMEs so this is hardly surprising. To understand that better, consider the following.

¹ <https://securitybrief.com.au/story/cyber-attacks-worsening-among-australian-businesses-costing-economy-1-billion-a-year>

- SMEs are unlikely to have dedicated IT staff
- SME's in-house IT team is unlikely to have the time to understand complex security procedures
- SMEs are likely to underestimate their risk

Here are some notable attacks on smaller players:

Hackers intercepted an invoice from an independent tradesman Simon O'Donnell. Scammers changed the bank details on the invoice and diverted \$51,000 into their account.

"Tradies frustrated by banks as business email scam costs them \$51,000" (Dec 1, 2020)
ABC News

The \$130 million wholesaling business had come to a screeching halt, placed behind lock and key after a hacker infiltrated its systems in a ransomware attack.

"They tore the heart out of my business": How a hacker nearly cost Gillian Franklin her \$130Million business (Aug 31 2020) - SmartCompany

Naturally, large businesses were hit just as bad.

Here are some notable cases:

MyBudget was hit by a ransomware attack. This caused a nationwide systems outage and 13,000 customers temporarily losing access to their accounts.

[MyBudget blames ransomware hack for system outage affecting thousands of customers. \(May 15, 2020\) - ABC NEWS](#)

Toll Logistics suffered two ransomware attacks in 2020 causing major issues such as downtime and data theft.

[Toll Group suffers ransomware attack again. \(May 8, 2020\) - Security Magazine](#)

Downtime like this can lead to a range of problems:

- Revenue loss
- Loss of reputation
- Lost employee productivity
- Customer dissatisfaction
- The cost of remedying the issue

As an MSP you're a target too

Criminals see MSPs as high-value targets. A popular tactic of theirs is gaining a foothold on an MSP's RMM. High profile examples have been a global, team effort, executed over many months. The MSP acts as the third party for hackers to gain access to. This gives the hackers access to the MSP's valuable customers such as government agencies or financial institutions. In the fight against cybercrime, the wise MSP knows that their security and their customers' security are one and the same.

The approach every MSP must take

Multi-layer security is what every MSP should strive for. This means going far beyond the usual: installing a firewall and ensuring multi-factor authentication is just the start. MSPs must ensure their customers are protected right down to the employee level as they are often the first line of defence. The Australian government reports that:

99% of cyber security incidents require human error to succeed.

Only **1 in 10** employees can explain cyber threat terminology such as malware, phishing, or ransomware.

ACSC Small Business Survey (July, 2020) - ACSC

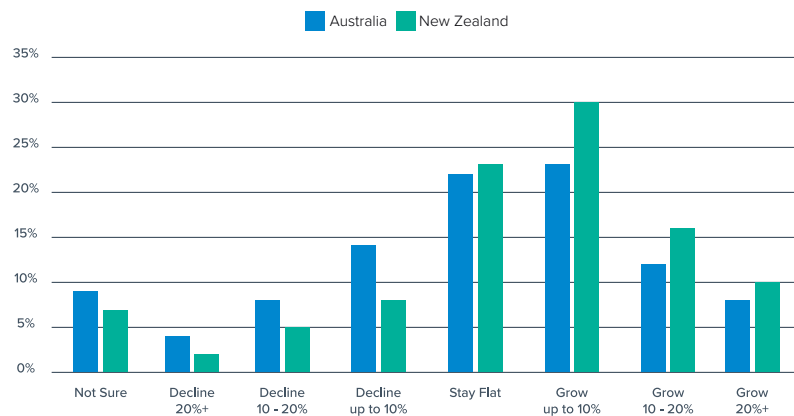


What does this mean for 2021?

Businesses are certainly feeling on edge and are starting to become more and more aware that their in-house IT staff lack the skills required to deal with these attacks. “Between 2017 and 2020, Australia’s cyber security sector revenue has grown by A\$800 million to A\$3.6 billion, with Australians spent approximately \$5.6 billion on cyber security from both local and international providers, with spending expected to increase to \$7.6 billion by 2024.” This trend aligns with the IDC’s ANZ SMB Survey, it says security revenue will climb to \$5.5 billion by 2024. New Zealand’s revenue also climbing within that timeframe to NZ\$821.

The following infographic offers a little more insight into how the security services market is set to grow over the next few years.

1 2020 Update to Australia’s Cyber Security Competitiveness Plan



% Respondents, N = 1210 SMBs in Australia and New Zealand
Source: IDC’s ANZ SMB Survey, October 2020

51% of Australian respondents indicated they would be spending more on IT this year. However New Zealand SMBs are not as optimistic with 43% of respondents doing the same.

COVID-19 is playing a large role in growing cyber security services

Emily Lynch, an associate market analyst for IDC ANZ has predicted that MSSPs will have the most growth across security-related services. It’s changed priorities for many businesses. In her words

“Organisations are facing additional challenges in maintaining their security environments. Working from home and remote learning expand the cyber-attack surface and exponentially increase the number of vulnerable endpoints.”

We should also bear in mind that the world economy is projected to pick back up in 2021. IDC projects global revenue for the IT industry to increase 4.2%. That will return the industry’s growth to where it was before 2020.

Here are 3 solutions that you will be doing more of in 2021.

The last couple of years have been a feast for cyber criminals

Remote work is here to stay. This means your customer's workforce will create a variety of endpoints, each with its own levels of (often questionable) security. To minimise your customer's security risk and make both compliance and troubleshooting easier, sufficient endpoint management will be vital. Educating end users on the importance of securing their endpoints themselves will also be wise.

Zero trust will become more popular

Some anti-virus solutions are beginning to stray from the "castle and moat" system thanks to cloud computing and remote work. Instead, they are using a system that refuses to grant access to IP addresses until they can confirm the user's identity and whether it's authorised. Here's Gartner's take on it.

"ZTNA is a technology that provides controlled access to resources, reducing the surface area for attack. The isolation afforded by ZTNA improves connectivity, removing the need to directly expose applications to the internet."

Security awareness training will be more important than ever

As touched on earlier, human error is the primary reason for most cyber-attacks. With fewer employees in the office using robust security technology, the only response is training them to be their own firewall and educating them on every aspect of cyber security that's beneficial for an end user to know. You have the opportunity as an MSP to be a trusted advisor to your end users and train them to be better at spotting phishing scams.

How to tackle your biggest challenges next year.

If you're like many other MSPs there will be certain challenges you're likely to face - regardless of a pandemic or any macroeconomic trend.

- Finding new business
- Selling cyber security
- Staffing issues

These will all need to be kept on top of in 2021. With those in mind, here are a few strategies for doing so.

Stand out by demonstrating specific vertical expertise

Victor Raessen, the man behind MSP Navigator, shared his thoughts recently. He advised that the MSP industry is 500,000 companies strong and growing every month. Many of them have little with which to differentiate from each other. Meanwhile, customers are still looking for a service – or at least an experience – tailored to their specific needs. Given all this, there's a sizable gap between what MSPs offer and what customers really want.

The smart MSP is the one that recognizes this. Even if it's just small tweaks, the MSP that demonstrates superior understanding of their customers' business and superior solutions guided by industry insight will stand out. This will help them win more business. In Raessen's words.

“You can keep the current building blocks that make up your tech stack, but the more you are able to add messaging that the customer recognizes, the more you increase your chance of success.”

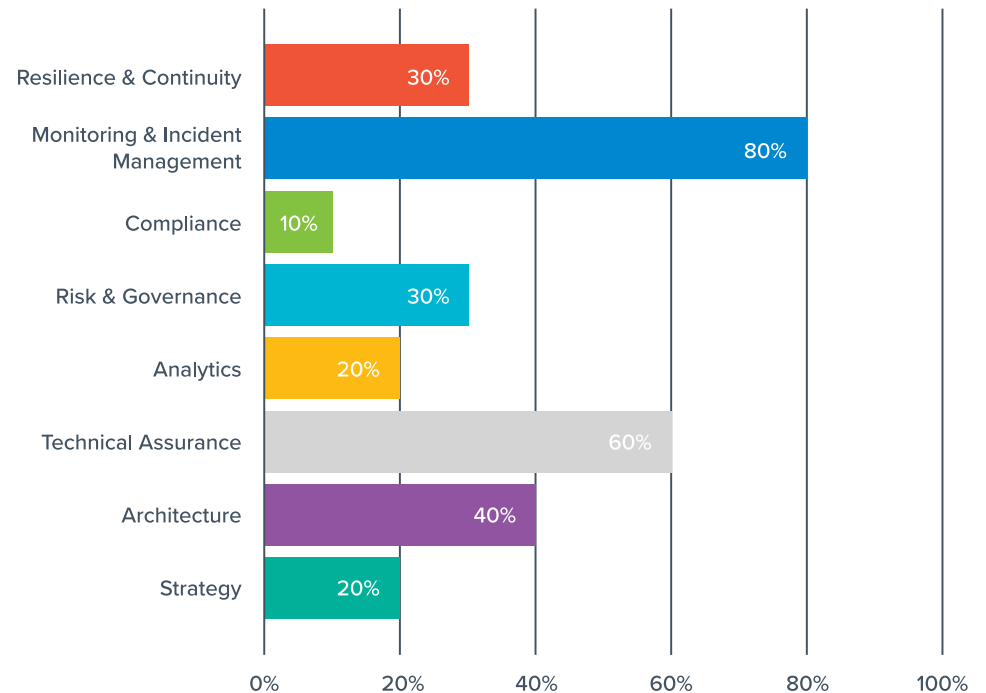
When it comes to solving business challenges, differentiation will help on the new business front. The more you can specialise, the further you move into a category of one, and the easier it is for customers to approach you. Also, the more you can demonstrate specific vertical expertise, the greater trust you can build with both prospects and current customers. This trust and industry specific knowledge can be used to both sell more services, cyber security certainly being one of them. One thing to note is that some verticals are more recession proof than others. Ideally you'll be able to strike a balance between “safe” verticals and expanding your market share into other territories that might be less safe.

Outsource and automate small, low margin services whilst focusing on the bigger more lucrative ones.

The real money for your MSP to make doesn't lie within basic connectivity services or standard IT support. It lies with high margin jobs such as managing compliance issues and cyber security. To focus on these more rewarding tasks, consider standardising, automating, and optimising the smaller tasks so that they take up less bandwidth. For example, taking a look at level one support tickets and possibly hiring new staff to keep small tasks away from experienced engineers can be hugely beneficial. Meanwhile, you can retrain and upskill your other staff so they're better equipped to solve bigger problems. With smaller tasks taken care of, you're now free to expand your service offerings and upsell these to your current customers and latest prospects.

Also, in upskilling your current workforce you can help fashion a more valuable and committed workforce that is more likely to stay with your business long term. It's also wise to combine this employee upskilling with new, innovative technologies to make your MSP as forward thinking as possible. This can help future proof both you and your customers making you more attractive to future employees and your current staff. The below graph from a recent AISA report offers a few thoughts on potential areas to upskill your workforce in.

Cyber Workforce Skills Deficiencies



Source: AISA Australian Cyber Security Skills and Jobs NSW Study 2020

Get better at showing your value

Value can be subjective, with multiple definitions. Sometimes it's as simple as showing a metric. On other occasions, it can only be demonstrated by building on your customer relationships and having long, transparent conversations with them. Value can vary from customer to customer. But either way, a number of principles will hold true.

- You're not selling services; you're selling the benefits those services bring
- Customers want to see ROI
- Our MSP should feel like a business partner to your customers

Before we outline how to demonstrate value, it's important to bear in mind these common pitfalls.

Mistaking your time for value:

Hours spent "busy" with customers don't necessarily equate to results.

Reporting without value:

Not all metrics demonstrate value. Make sure the metrics you report do.

Letting reporting go to waste:

Don't just send a report along with the monthly bill and leave it open to interpretation.

Overtreating a new customer:

Once the service and attention that comes with onboarding wane, the perceived value of your service may follow.

Customer misalignment:

Your customers' needs can change. You must remain aware to ensure your services carry on meeting them.

Here are five ways your MSP can demonstrate its value better.

Schedule periodic customer meetings

You don't want to get into an out of sight, out of mind situation. Schedule regular meetings to keep everyone aware of the past, present, and future value delivery. Ideally these will be done in person. Once a quarter is typically a sweet spot, however, this may vary depending on how long it can take to see value. The meetings should cover topics such as:

- Current state of the customer's environment: what state are your customers' IT systems currently in?
- Reporting to reflect and visualise value delivered
- Educating your customers on cyber security
- New services: given the outcomes of the past quarter, what more can be offered by the MSP?

Deliver value driven reports

These can't just be a bunch of incomprehensible numbers and graphs. These need to be – for want of a better word – idiot proof presentations for seeing the success of your services at a glance. As mentioned earlier, these figures must indicate relevant value. A customer doesn't want to hear about how much time their employees spend using Microsoft Teams. They want to see metrics that indicate how well, or how badly their IT is impacting things like their security or their bottom line. To ease your customer into such assessment, Barracuda MSP has several complimentary tools for IT service providers to use, such as the [Email Threat Scanner](#) and [Web Applications Scanner](#).

Treat every customer like they're new

The service and willingness to impress that can often be found at the beginning of a customer relationship needs to become the norm. Make sure you spend quality face time with every customer in equal measure no matter how long you've been working together.

Frequently communicate with customers

Aside from quarterly meetings, make sure you stay in regular contact with your customers. Both to keep on top of issues and reassure them that you're delivering the value you promise. Not every interaction even needs to be business related either. Sometimes it's great to just check in to see how things are going.

Have a value centric service level agreement

Make sure your SLA doesn't just focus on the levels of services provided. Make sure it emphasises the value these services bring. Choose the right metrics to show and even consider adding additional information to educate your customer on its value if need be.

When you demonstrate value and a reason to believe in your MSP's expertise, winning more business – be it via upselling or from new customers – becomes easier. With concrete evidence that your MSP service does what your customers want from it, you remove the risk and anxiety that a customer may feel before purchasing. For this reason, demonstrating value will also help you sell more cyber security.



There is one last business challenge you may not have considered.

As an MSP you're in a prime position for falling victim to a cyber-attack. Why wouldn't you make sure you're cyber secure before accepting the keys to your customer's kingdom?

In the wake of several attacks on Australian and global MSPs, Alistair MacGibbon, former Head National Cyber Security Adviser and Australian Cyber Security Centre had this to say on ABC radio at the end of 2018.

“These managed service providers as trusted IT providers for companies and governments around the world have unique access, and once they are compromised... they can gain access to commercial secrets.”

Alistair MacGibbon, former Head National Cyber Security Adviser and Australian Cyber Security Centre

Since criminals can leverage the existing trust and relationships between MSPs and customers they can gain access to MSP's networks. Hence why a 2019 report by the Australian Cyber Security Centre also declared that.

“MSPs are attractive targets for state actors and cybercriminals”. With so much of their work being performed remotely, cyber criminals see MSPs as a golden opportunity. Elaborating further, Juan Fernandez the vice president of managed IT services at ImageNet Consulting, an MSP in Oklahoma believes the collective value of an MSP's customers can be greater than that of a large business. In his words.

“Data is the new gold rush. All of a sudden, there are a lot of SMBs with important data and they're not as protected... The bad guys think ‘forget those big guys, I'm going to get a bunch of small ones and make some money.’”

Juan Fernandez, VP of Managed Services, ImageNet Consulting

Combine the above with the fact that the consequences can also be pretty dire for the unlucky MSP. Since MSPs are engaged as a secure IT and business partner, both their customers' and their own reputation is very much on the line at all times. So what's the solution? Partnering with a company that can specialise in cybersecurity whilst building your own cyber security skills in the meantime.

Preparing for 2021 may seem like a big task.

Simply making it through 2020 has been challenging enough for most businesses. Many of us are still licking our wounds, and the thought of attacking next year might feel uncomfortable. But when we break down what can be done the future feels a little more manageable. Tackling as many of the seven points to the right will stand you in good stead.

The final point is one to take particular note of. In partnering with a vendor that really understands cyber security, many of the other six points can be taken care of more easily. For example, things like security awareness training and a focus on more lucrative services (such as cyber security) can be addressed more easily. With a dedicated cyber security expert as part of your MSP, you'll also stay abreast of new developments and have more bandwidth to tackle everything 2021 might throw at you.

If you'd like to make 2021 the year your business maximises its potential and stops every cyber threat in its path, [click here](#) to speak with a BarracudaMSP representative today.

Email: APACMSP_Team@barracuda.com **Tel:** +61 1300 431 470



Optimising endpoint management



Employing Zero Trust technology



Rigorous security awareness training



Demonstrating your vertical expertise



Streamlining low margin services whilst focusing on the larger, more lucrative ones



Demonstrating your value



Partnering with a vendor that really understands cyber security