HostedNetwork | Whitepaper

MSP Cyber Security Playbook

Introduction

You've worked hard to gain your customers' trust. But with that comes responsibilities – to your customers as well as your business and its stakeholders.

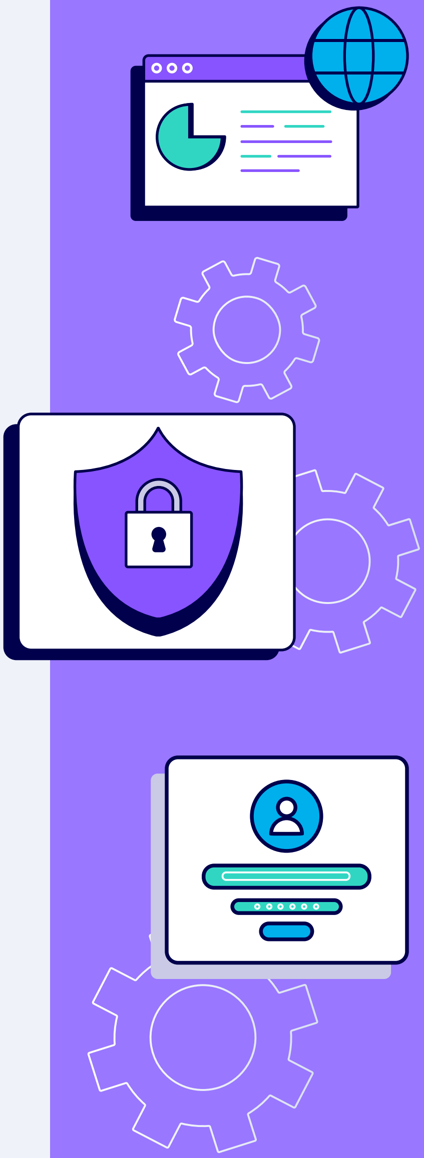
As an MSP, you've played a key role in helping your customers maximise their business productivity and continuity. But now, you find you're also expected to provide them with the specialist services needed to remediate the risk and impact of a cyberattack.

This means that, like it or not, you need to be across everything cyber security. Because if you aren't, you can guarantee your competitors will be.

We know that getting your head around managing someone else's risk can be daunting. And that lack of certainty and knowledge can potentially endanger your customers' businesses and your own.

It's equally important to consider the impact of offering cyber security services on your own business growth and operational maturity. Adding cyber security to your services mix serves as both an opportunity to drive greater profitability while strengthening your ability to compete effectively in a customer-hungry market, as well as a necessity to protect your capability to deliver existing managed service offerings.

So, this whitepaper is designed to guide you as to how you can introduce, round out, or strengthen your cyber security capabilities and, in doing so, live up to some pretty big customer (and your own stakeholder) expectations.



What makes a great MSP?

Doing an exceptional job of securing your customers' businesses is key to being the best possible MSP.

Your customers rely on you for business continuity. Their apps, systems, devices, networks, and everything else that enables them to operate all depend on you. As a true business partner, you're also the gatekeeper of their entire technology environment. You are responsible for keeping the bad guys at bay, regardless of how and where they launch their attack from.

Just as strata management protects all the tenants and their amenities in the building they share, a great MSP ensures that the doors, smoke and burglar alarms, cameras, and evacuation processes work. Without fail.

Why every MSP needs a cyber strategy for their clients

Today's customers assume that you're taking care of everything MSP – and that you are a great cyber security allrounder. They trust you to secure their systems and data by providing the latest and best services and technologies. To keep them ahead of the tsunami of cyber threats and out of harm's way. And if they are impacted, to guide them through a well-orchestrated journey of remediation and recovery.

So, no pressure. After all, it's only your reputation that's at stake.

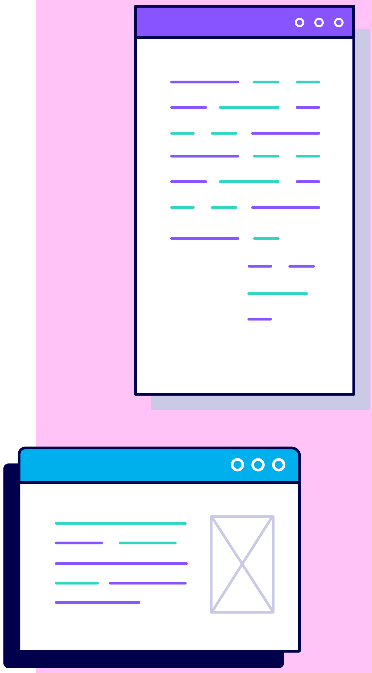
However, if you're still at the antivirus and firewall end of the cyber security game, you've got a problem. They're no longer enough to keep your customers safe (or impress them) - and haven't been for some time.

While we always talk about the importance of cyber security strategies for our customers, as an MSP, you also need your own strategy to deliver what's needed. After all, your own offerings and approach will be under the microscope.

Are you in the line of fire in a customer data breach?

Yes. The reality is that following the changes to the Australian Privacy Act in 2022 if you manage a customer's data, you could be found liable in the case of a cyber incident.

If you think that doesn't sound like 'a thing' in Australia, then the Medibank breach should make you think again. Medibank's IT provider was named in the wake of the health insurer's highly publicised breach in 2022. While the IT provider wasn't found liable (and the breach occurred before the Privacy Act 2022 changes), the expectation moving forward is that Australian MSPs will be held to account for their role in any data breach.



What are the benefits of offering a full cyber security offering?

As organisations move towards integrated security solutions, they're increasingly seeking out MSPs who can handle everything from threat detection to incident response. While this means the pressure is on you to perform, it also means your customers have no need to look elsewhere, making it a significant opportunity to build trust, extend relationships, and grow your business.

So, what are the benefits of selling, deploying and managing cyber security services for your customers?

1 **Defend with vigour:** Protect your customers and your own business from the ever-evolving threat landscape with more confidence.

2 **Increase your insurability:** Meet all the criteria required to obtain MSP cyber insurance, including demonstrating you have strong cyber security practices and documented policies and procedures.

3 **Enable regulatory compliance:** Offering the full range of cyber security services can help you and your customers remain compliant in the face of strict regulation regarding data protection and cyber security - avoiding potential fines and legal ramifications.

4 **Tick the integration box:** A fully integrated cyber security offering ensures all your security tools and strategies work seamlessly together. This enhances the overall effectiveness of your security measures and reduces those hacker-prone gaps.

5 **Offer a more cost-effective suite of services:** Your security offering will be more competitive when compared with the time, cost, and effort it takes your customers to manage multiple vendors.

6 **Build trust:** Businesses are more likely to partner with MSPs that demonstrate a robust and proactive 'all-in' commitment to security. This includes identifying and mitigating potential threats, continuous monitoring, vulnerability assessments, and regular security updates.

7 **Develop your operational maturity:** By investing in cyber security, you strengthen your own security practices, improve risk management, increase your service offerings and capabilities, and foster a culture of continuous improvement. The outcome? You'll enjoy better customer relationships, improve operational efficiency, and achieve a stronger competitive position in the market.

8 **Grow your profitability:** Not only will a full suite of cyber security services attract new customers, but it will also delight those who already count on you for other managed services and don't want to engage yet another IT partner.

9 **Be a true MSP:** At the end of the day, it's your job as an MSP to provide performance and continuity to your end customers' businesses (you keep their business running). A security incident could quickly undermine your perceived value and ruin your reputation.

What does a robust cyber security posture include?

- ✓ Risk management
- ✓ Incident response
- ✓ Compliance and governance
- ✓ Security architecture
- ✓ Employee training and awareness

It also takes into account the following types of cyber security technologies:

- ✓ Network security
- ✓ Cloud security
- ✓ Endpoint security
- ✓ Mobile security
- ✓ IoT security
- ✓ Application security
- ✓ Zero trust

What stops some MSPs from taking on cyber security?

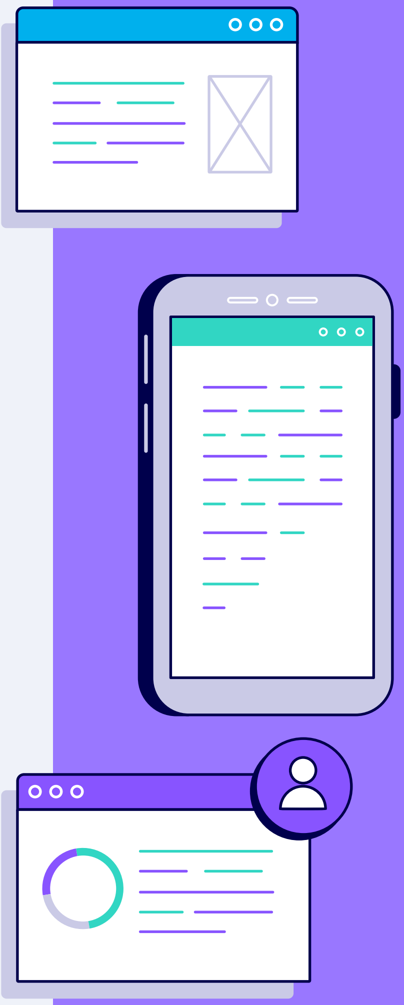
Many of the same challenges that make customers question the advisability of taking on the challenge of cyber security internally, are also faced by MSPs.

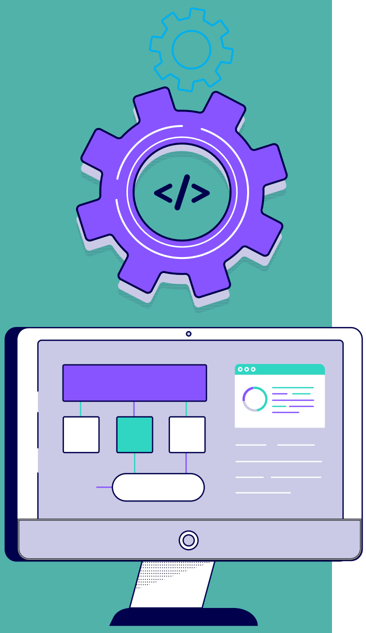
One major challenge is being unable to find, afford, and retain trained and experienced resources. And you can't take any shortcuts or learn on the job. Cyber security is a highly specialised field requiring specific knowledge and skills. So, managing and maintaining the complex solutions and services needed to constantly improve your security posture without enough knowledge can be daunting.

And then, there's the very real (and sensible) fear of risk. Cyber security often involves navigating complicated compliance requirements and keeping pace with the latest developments and best practices. The challenge of keeping up with regulations like GDPR, the Privacy Act, or PCI-DSS is a deterrent to many MSPs entering the cyber security space.

Equally, the investment cost in cyber security tools, technologies, and training can be substantial and equally off-putting if you're unsure about the return on investment.

However, the cyber landscape also offers an opportunity to grow your business and increase your profitability significantly. And it's not one you should walk past without careful consideration.



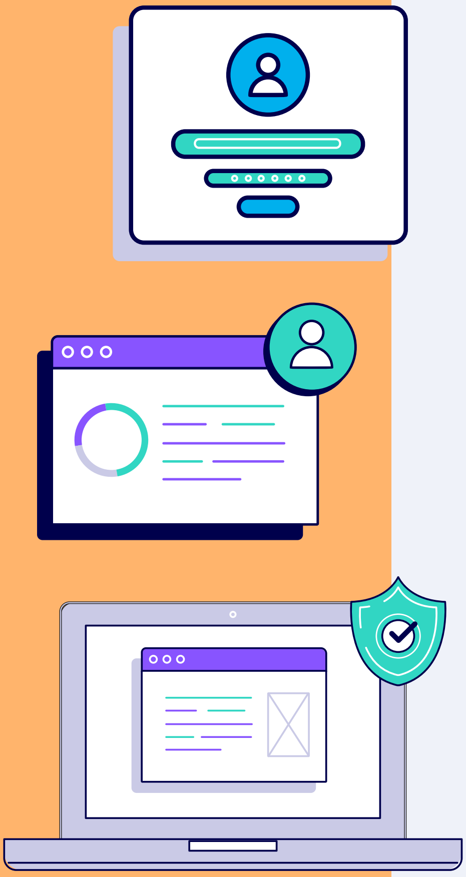


Exactly how short-skilled is the Australian cyber security industry?

In short: very.

According to the 2023 AustCyber's Cyber Security Sector Competitiveness Plan, 74% of security professionals reported a significant lack of qualified workers. While there were 51,309 dedicated workers in cyber security in Australia in 2023, there were also 12,500 unfilled vacancies.

AustCyber says that the cyber security workforce needs to grow by 66% to reach the 85,000 required by 2030. That's more than 4800 jobs every year.



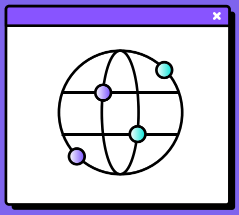
The risk-free approach to becoming a full cyber security service MSP

Just as your customers outsource their managed services to you, you can outsource your cyber security services to trusted specialists. This enables you to be the security expert your customers expect you to be without adding expense to your business.

Why outsource? Outsourcing your cyber security services allows you to:

- Upsell and cross-sell services to your customers without going to the effort and expense of increasing your own headcount.
- Free up billable hours for what you do best and most efficiently.
- Sleep soundly at night knowing your customers are protected 24/7/365.
- Leverage the expertise of people who specialise in threat hunting and mitigating advanced attacks and breaches and can provide AI-led threat intelligence.
- Provide round-the-clock ransomware and breach prevention services to minimise the impact of a cyber incident (the longer an attacker is in a system, the more damage they can do).
- Concentrate on your MSP business, knowing your customers are in good hands. All their alerts are being actively monitored, prioritised and actioned day in and day out by security experts while it's BAU for you and your team.

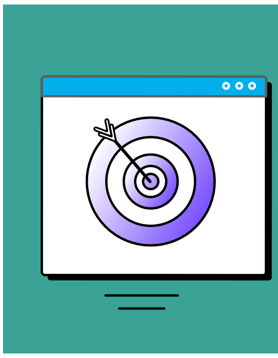
The 4-step start:



1. Select a SOC

First, choose a managed SOC (security operations centre). Look for one that is exclusively designed to support how MSPs work and do business, and offers:

- A straightforward monthly billing structure
- Service-based pricing (so user pays)
- Competitive pricing with high margins
- The ability to maximise your ROI by integrating with tools and other security products you already own



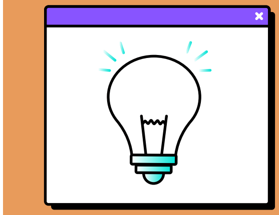
2. Choose your approach

Then, decide whether your business will be best served by consolidating all your cyber security tools in a single platform – or not. There are pros and cons either way, which requires you to carefully evaluate your specific needs and circumstances before deciding.

Pros of consolidating on a single platform	Pros of not consolidating
Simplified management to minimise effort: A single platform can streamline your administration, making it easier to manage and oversee security efforts without juggling multiple tools and interfaces.	**Retain best-of-breed preferences:** A single platform may not offer the specialised features or capabilities of dedicated tools, potentially limiting its effectiveness in certain areas of cyber security.
Supercharged response times: Tools that are part of a unified platform are often designed to work together seamlessly – enhancing data sharing and communication and resulting in faster response times.	**No vendor lock-in:** Consolidation on a single platform may lead to dependence on a single vendor, making it difficult to switch providers or incorporate best-of-breed tools in the future.
Keep costs down: Consolidating tools can drive down the costs associated with licensing, maintenance, and training due to reduced vendor management overheads.	**No single point of failure:** Relying on one platform can create a vulnerability. If the platform is compromised or experiences downtime, it could expose all your customers to risk.
All data in one place: With centralised security, data analysis and reporting are easier, faster and more comprehensive. So, you have an unobscured view of any customer's security posture.	**Maximise existing resources and efficiencies:** Consolidating tools may lead to redundancy, where multiple features or functionalities overlap, and devaluing those tools you already have.
Better visibility: A unified platform will provide a holistic business-wide view of security, helping to identify vulnerabilities and cyber threats more effectively.	**Drive value from existing tools:** Maximise your ROI by integrating tools and other security products you already own and understand.
Streamlined incident response: With all tools integrated, incident response can be faster and more coordinated, reducing the time it takes to detect and mitigate threats.	

Not sure which way to go?

MSPs using multiple platforms estimate they would save an average of **48%** of their day-to-day management time by managing all their cyber security tools from a single platform.



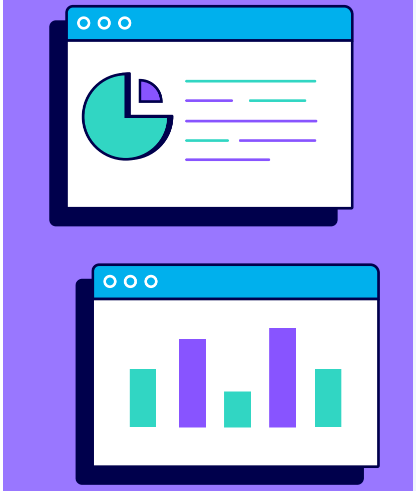
3. Get to know your customers' strengths and weaknesses

Next, take the time to understand your customers, their systems and their requirements. No two customers are the same; each has their own complex technological infrastructure, networks, systems, applications, endpoints, processes, and requirements.

4. Educate and train

Lastly, educate your customers about the threat landscape.

Cyber security awareness is key to their appreciation of the strengths or weaknesses of their security posture, new and emerging threats, and fostering a culture of security within their business – from adopting strong password practices and safe browsing habits to recognising social engineering and identity theft techniques, and more.



Summary

As an MSP, the seemingly unstoppable rise of cybercrime presents your business with significant opportunities to compete and grow. Not only can you enhance your service offerings without increasing headcount, but you can build stronger and more loyal customer relationships, attract new customers more easily, and increase your revenue.

By positioning yourself as a trusted cyber security partner, you'll help your customers navigate the complex threat landscape as well as secure their own growth and success in the market.

And that makes becoming a managed cyber security partner a win-win for everyone except the criminals.

Ready to take the next step in your MSPs cyber security journey?

To learn more about how Hosted Network can help you with your cyber security needs, get in touch with us via phone at **1300 781 148** or email us at **sales@hostednetwork.com.au**