+44 345 094 0945
www.waterstons.com

Article

Sep 2024

How a SOC Can Help SME's Punch Above Their Weight in Cybersecurity

In this must-read breakdown, discover why hackers are targeting SMEs, the high price of unprotected data, and how a 24/7 Security Operations Centre could be the game-changer your business needs to stay secure.



Oliver Baverstock
SOC Team Lead
Email oliver.baverstock@waterstons.com





Australia's SMEs are under siege—cyberattacks now hit every 10 minutes, and 60% are aimed at small to medium businesses. With attack costs reaching up to $97,000, the fallout from just one breach could cripple your operations. In this must-read breakdown, discover why hackers are targeting SMEs, the high price of unprotected data, and how a 24/7 Security Operations Centre could be the game-changer your business needs to stay secure.

The Current Cyber Landscape for SME's

Cyber threats have increased dramatically in the last 5 years and continue to rapidly evolve, increasing in frequency and complexity. Every Aussie business has been or will be affected by a cyber threat during their operations.

SMEs, often operating with limited resources, find themselves particularly vulnerable to these evolving threats, leaving them exposed to ransomware, phishing attacks, and Business Email Compromise (BEC) schemes.

Key SME's Cyber Stats:

- 60% of cyber-attacks are targeted at SME's
- Every 10 minutes a cyber-attacks occurs in Australia
- Average cost of cyber crime is between $46,000 and $97,000 depending on the size of your business

We could inundate you with countless statistics, but these figures alone highlight the urgent threat cyberattacks pose to SMEs. However, fear isn't our goal—awareness is. We aim to shed light on this ever-evolving issue and empower your business to stay ahead of it.

With new legislation on the horizon, imposing tougher fines and penalties for non-compliant organisations, Australia is taking a decisive stance against cyber threats.

The cost of a breach—both financial and reputational—can be devastating. But your organisation doesn't have to be the next target.

Why Your SME is an Attractive Target for Hackers

Hackers are opportunistic criminals.

SME's are attractive to them for several reasons.

- Many SME's lack the same robust cybersecurity posture which larger corporations have, making you easier to breach.
- Your organisation more than likely possesses valuable information such as financial or personal information of your stakeholders, making a data breach highly lucrative.
- SME's frequently serve as supply chain partner for larger companies, hackers can often view your business as a stepping stone to a larger fish.

Perceived lower security investment paired with valuable data have turned SME's into a goldmine for these criminals.

Minimising Your Downtime + Operational Disruption

One of the most significant risk of a cyberattack on your organisation is the potential for operational disruption. Delays in stakeholder service, extended downtime, reputational damage are a few of the consequences of suffering an attack. the fallout can be devastating—especially for SMEs.

Without the resources to absorb these losses, even a single attack can heavily impact your bottom line and erode customer trust.

The Tale of Terry and Tony: A Case Study on Cybersecurity for SMEs

Terry's Meats takes cybersecurity seriously. With a 24/7 Security Operations Centre (SOC) and strong cyber hygiene practices throughout his organisation, Terry understands the modern threat landscape well enough to know that partnering with a reputable cyber expert is key to keeping his small business safe.

Tony's Meats, on the other hand, does not have a 24/7 SOC or comprehensive cybersecurity practices in place. While Tony is aware of the growing cyber threat, he assumes his business is too small to be a target.

Both Terry and Tony fall victim to the same phishing email scam. Unfortunately, both accidentally click the malicious link, triggering a ransomware attack on their systems.

For Terry, the response is swift. His trusted cyber partner detects the breach almost instantly, activates the incident response plan, and works to contain the damage.

Tony, however, is not so fortunate. His systems are immediately locked down, hackers demand a $25,000 ransom, and Tony finds himself unable to operate. He can't manage staff schedules, fulfill orders for his suppliers, or even access his payment terminals. His business grinds to a halt.

Terry's Outcome

Within 48 hours, Terry's Meats is back up and running, thanks to the swift action of his SOC. He receives additional training for himself and his staff on recognising phishing scams, and his cyber partner delivers a full report on the incident.

Tony's Outcome

Within the same 48 hours, Tony's Meats is still crippled. His financial losses are mounting, downtime persists, and his suppliers and stakeholders are now looking for more reliable partners. Eventually, Tony pays the ransom but still faces the aftermath—he must change all his passwords and bank accounts, and spend an additional $15,000 to fix the damage. In total, Tony is out $40,000, but that doesn't account for the loss of contracts and stakeholder trust.

The Final Chapter

Two weeks later, Terry has absorbed most of Tony's business, expanding his operations and reinforcing his position as a trusted supplier. Tony, meanwhile, lost most of his clients, his reputation in shambles, and his business struggling to recover.

Lesson Learned

This case study highlights a simple truth: SMEs must invest in cybersecurity. Without it, the cost of an attack could far outweigh the investment in protection. In today's threat landscape, no business is too small to be a target.

SOC: Enterprise-Level Protection, Without the Enterprise-Level Cost

A 24/7 SOC is Essential.

This complex threat landscape requires proactivity, not reactivity.

A Security Operations Center (SOC) that provides 24/7 monitoring is no longer a luxury organisations can afford not to have- it's a necessity.

Not all SOC teams are created equal. A great SOC team will be continually and proactively scanning for suspicious activity, responding to threats in real time and work to mitigate damage before it spreads.

Having a dedicated SOC team on your side ensures protection for your organisation around the clock, 365 days a year. Ensuring no breach goes undetected.

An excellent SOC and cyber partner should also be...

- Keeping you updated on the latest threats

- Provide actionable advice for an improved cyber posture
- Provide proactive monitoring 24/7, 365 days a year
- A personalised and bespoke service based on the needs of your business
- Save you time, money and headaches through their service

An excellent SOC doesn't have to break the budget either. Every organisation should have cyber protection. Which is why our SOC service is priced to accommodate for most businesses budget.

Key Takeaways

SMEs Are Prime Targets for Cyberattacks

SMEs are increasingly targeted by cybercriminals due to perceived lower cybersecurity investments. Attackers find SMEs attractive for the valuable data they hold and their role in larger supply chains.

The Growing Threat and Its Impact

Cyber threats have escalated in complexity and frequency over the last five years. With 60% of attacks aimed at SMEs and incidents happening every 10 minutes in Australia, the financial and operational consequences can be devastating, averaging between $46,000 to $97,000 per incident.

The Importance of Cyber Hygiene and 24/7 Monitoring

SMEs that invest in good cybersecurity practices, such as 24/7 Security Operations Centres (SOCs), are better equipped to handle cyber threats. Real-time threat detection and response can prevent prolonged downtime, financial losses, and reputational damage.

Regulatory Compliance and Competitive Advantage

With tougher legislation and fines for non-compliance on the horizon, investing in cybersecurity not only ensures regulatory compliance but also gives SMEs a competitive advantage by building customer trust and safeguarding operations.

Investing in Cybersecurity Is Essential

As shown in the case study of Terry and Tony, the consequences of not investing in cybersecurity can be severe, leading to business failure. A proactive cybersecurity approach, especially a managed SOC, can save SMEs from crippling losses and help them thrive in a hostile cyber environment.

If you would like more information about our SOC, get in touch below for an obligation free vulnerability assessment.

Info@waterstons.com | + 02 9160 8430

Appendix

https://au.marsh.com/products-services/cyber-insurance/insights/increasing-cyber-attacks-australian-small-medium-enterprises.html#:~:text=On%20average%2C%20there%20is%20a,the%20most%20targeted%20area3.

https://leapstrategies.com.au/the-rising-tide-of-ransomware-and-targeted-cyber-attacks-on-smbs-in-2023/#:~:text=Types%20of%20Targeted%20Cyber%20Attacks,small%20and%20medium%2Dsized%20enterprises.

https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/small-business-cyber-security