



Overcoming the '*I'm Too Small to be Hacked*' Illusion: Cybersecurity Essentials for Australian SMEs



Introduction

Cybersecurity is a growing issue across Australia, impacting organisations of all sizes. In recent years, cyberattacks have become more automated, sophisticated, and frequent, affecting companies in every industry.

In its most recent report, the ACSC published some alarming figures, showing that the frequency of cybercrime increased by 13% from 2021 to 2022, while the cost of each incident also increased by 14%. The average cost per cybercrime report increased to over \$39,000 for small businesses, \$88,000 for medium businesses, and over \$62,000 for large businesses¹.

Unfortunately, this means the mentality of *'We're too small to be hacked'* no longer holds true and can lead to costly and brand-damaging cyber incidents, which can have devastating effects on small and medium-sized businesses.



Targeting of Cyber Attacks

The mentality of *'We're too small to be hacked'* comes from a view that cybercriminals pick their targets based on the biggest possible payday and thus target large organisations with deep pockets. Unfortunately, this is simply not true.

In the same way that small businesses don't start out by looking for multi-million-dollar deals, cybercriminals rarely look for the biggest possible payday. The vast majority of cybercriminals don't have the skills necessary to carry out Hollywood-style hacking attacks on large organisations with

strong cyber defences, so instead, they target smaller organisations with defences that are easier for them to breach. Often, even advanced cybercriminals seek smaller and more regular successful attackers over larger, complicated attacks that take longer for them to carry out and have a lower success rate.

Put simply, most bank robbers aren't targeting Fort Knox. Similarly, most cybercriminals aren't targeting large multi-nation organisations.

¹<https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022>

Automation and the Scatter Gun Approach to Cyber Attacks

With the development and proliferation of scanning technologies, cybercriminals no longer pick a target and work their way through its defences; instead, they scan hundreds of potential targets per second and select those with the weakest defences. The internet connects billions of people worldwide to every business, and scanning technologies make it easy for bad actors to find businesses with weak defences.

This becomes more of an issue when attackers use tools 'cybercrime as a service' tools. Modern attackers don't need significant knowledge of breaching computer networks. Instead, an underground ecosystem facilitates the sale and purchase of tools created by more sophisticated cybercriminals. This allows cybercriminals with even a limited knowledge of computer security to mount attacks. They scan the internet for networks with known vulnerabilities, then use their cybercrime as a service tool to begin an attack.

Ultimately, many cybercriminals select their targets based purely on how easy they are to breach, without any consideration of the business's size.

This means that small and medium-sized businesses are targeted as much, or even more so, than large businesses with large cybersecurity budgets, contrary to the 'We're too small to be hacked' mentality.

This is most often seen in phishing attackers. Attackers don't often pick a single target and launch a phishing attack against them. Instead, they send millions of phishing emails at once to potential targets in a scattergun approach. They send phishing emails to individuals, small businesses, and large businesses all at once and see which ones are susceptible to becoming victims.



How to protect a small or medium-sized business

All businesses face budgetary challenges, which means the biggest cybersecurity issue SMEs face is how to get the best defence with a limited budget.

To do this, a business must first understand the risks it faces. It can be easy to grab the latest cybersecurity solution with all the bells and whistles, but SMEs must be laser-focused on investing in the solution set which mitigates their specific risks and provides them with the best return on their spending. To do this, they must first know what risks they face.

A great place to start is the Australian Government's Essential Eight framework. These are the eight cybersecurity strategies that the Australian Cyber Security Centre

(ACSC) defines as the most important of their complete set of thirty-seven mitigation strategies.

The Essential Eight serves as a simple starting point for small businesses to embark on their cybersecurity journey and helps all businesses prioritise their spending on cybersecurity. The Essential Eight includes three maturity levels to support the eight mitigation strategies. SMEs can select based on their risks and likelihood of being attacked. This helps ensure a holistic approach to cybersecurity, resulting in broad defensive coverage rather than over-investing in one area and leaving others unprotected.

Working with Partners

A key challenge for SMEs beginning their cybersecurity journey is selecting the right tools. There are thousands of cybersecurity solutions available on the market which seek to mitigate different risks in different ways. For businesses with internal cybersecurity expertise, working directly with vendors to procure the tools they need for their specific risks can be an effective strategy, but when internal expertise is limited, SMEs need to work with an expert partner who can ensure

they get the right mix of cybersecurity tools for their unique risks.

Solution vendors will always find a reason why an SME needs their specific tool, while partners will work with SMEs to understand their risk profile and budget and implement the right most possible risk reduction for the budget available.

Conclusion


Being small is no longer a protection against cyberattacks. In recent years cyberattacks have become easier to launch and more automated. This has resulted in targets being selected based on how easy they are to penetrate, not the potential payoff after a successful breach. Owners of businesses of all sizes must prioritise cybersecurity, taking proactive measures to protect their businesses from the devastating consequences of a security breach.

By taking a risk-based approach and investing in defences that mitigate their specific risks, SMEs can achieve a better return on their cybersecurity investment and, ultimately, a cost-effective cyber defence.





Contact info

 1300 348 287

 hello@emergeit.com.au

 www.linkedin.com/company/emerge-it-solutions-pty-ltd