PREMIER
Technology Solutions

Australian Cyber Security Insights for the SMB Market

THOUGHT LEADERSHIP

INTRODUCTION

Cyber security threats are becoming an increasing concern for businesses. This paper looks into recent trends on where cyber security breaches of Australian organisations are originating, breaks down why Australian businesses are prime targets, and provides recommendations on some simple steps that can be taken to reduce the risk.

Current Environment

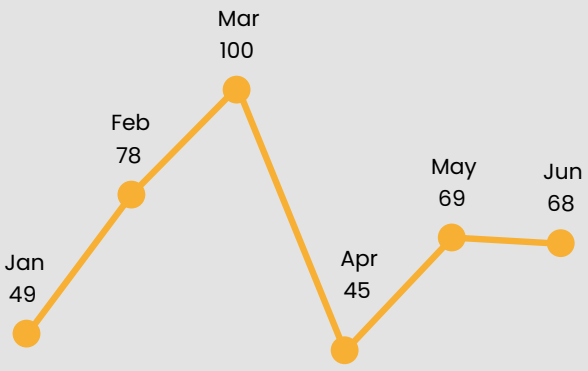
A recent OAIC (Office of the Australian Information Commissioner) report looking at information breaches in the first half of 2023 found that 70% of breaches were from malicious or criminal attack, a further 26% from human error and the remainder from system faults.

Organisations should assume human error will occur and design for it. The OAIC encourages the embedding of good privacy practices into all functions and activities. This includes designing systems and processes that anticipate and minimise the risk of human error.

Snapshot

409
notifications

Down 16%



WHY WOULD I BE A TARGET?

The Australian Signals Directorate (ASD) report that the cost of cybercrime in FY23 for small business was $46,000 and the cost for medium business was $97,200. When compared to the average annual salary of $40,000 in the four countries believed to be the origin of most attacks (Russia, China, North Korea & Iran), the ROI for targeting SMBs with typically low cyber security defences becomes a no brainer.

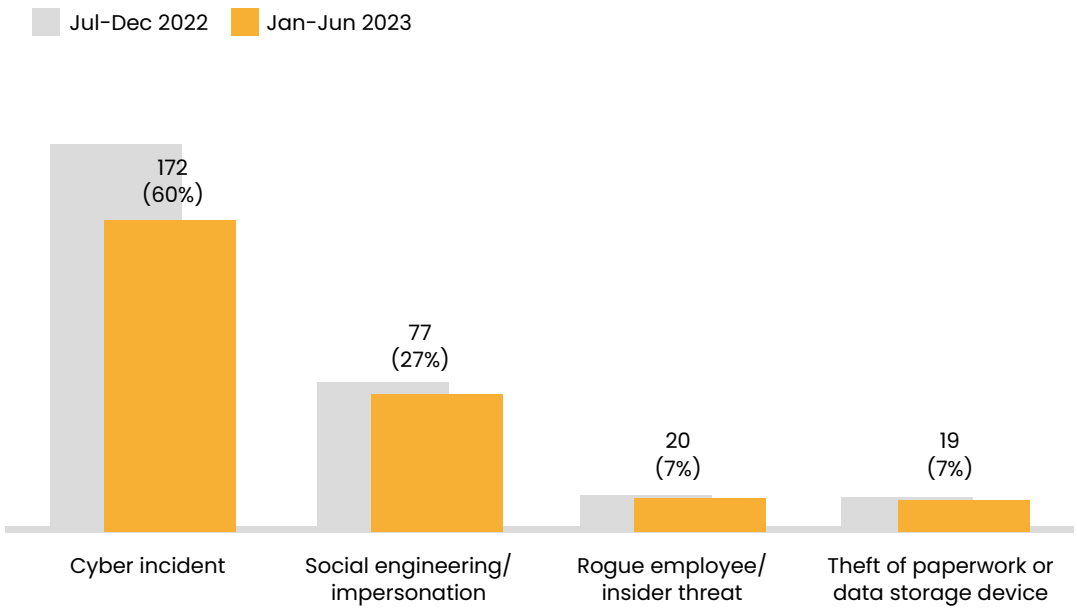
The ASD received 94,000 cyber crime reports in FY23, an average of one report ever six minutes, making a breach a question of when, not if.

KEY TAKEAWAY

Cyber-attacks resulting in actual breaches for SMBs are numerous and businesses need to assume they will be breached at some point and have a mitigation plan in place.

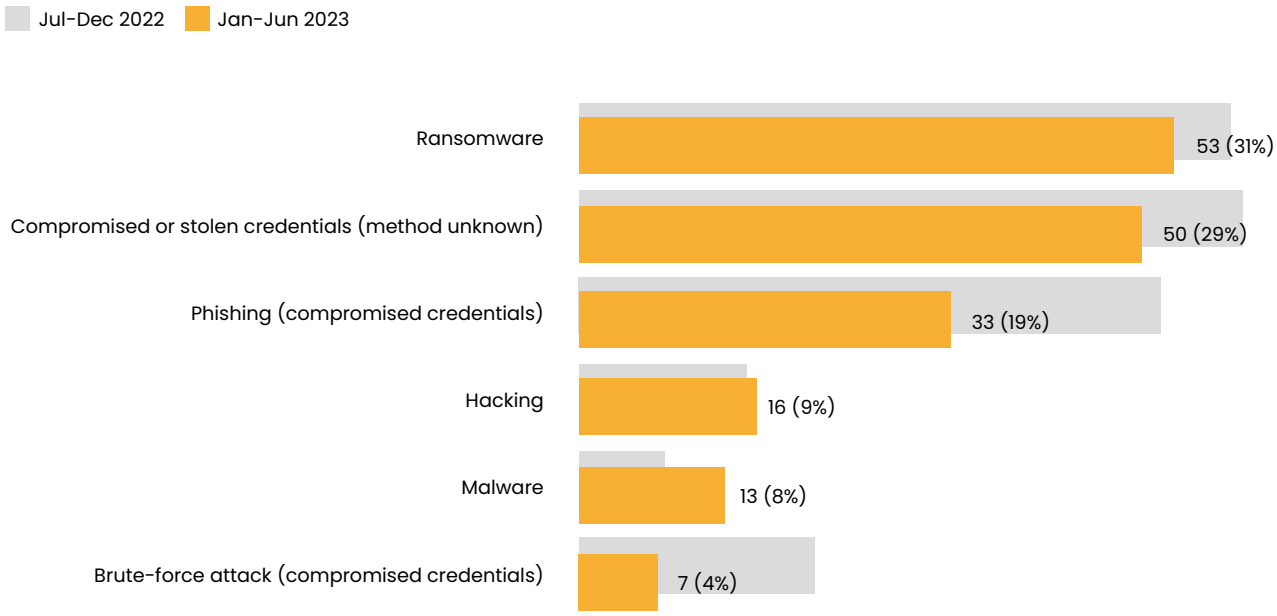
MALICIOUS OR CRIMINAL ATTACKS

60% of malicious breaches were caused by cyber incidents (breakdown below). With the remainder split across social engineering or impersonation (27%), actions taken by a rogue employee or insider threat (7%), and theft of paperwork or data storage device (7%).



This means that nearly 1 in 5 of all data breaches were caused by social engineering or impersonation. This highlights the importance of remaining vigilant to these attacks, as threat actors use increasingly sophisticated methods to gain trust, bypass authentication measures, and access accounts.

Ransomware remained the number one source of cyber incidents, followed closely by compromised or stolen credentials, then phishing attacks.



KEY INSIGHT

Remain vigilant to social engineering and impersonation.

RECOMMENDATION

Ensure cyber security onboarding and end user training is in place, and enable multi-factor authentication on all systems.

THE MOSAIC EFFECT IS A GROWING CONCERN

Recent large-scale data breaches have created the potential for a mosaic effect. A mosaic effect occurs when separate pieces of information, collated from various sources, including the dark web, are combined to create a more comprehensive understanding of individuals or groups. This equips threat actors to impersonate multiple individuals, gain trust and circumvent authentication measures to access accounts.

With this capability and knowledge, threat actors are more adept at accessing multiple systems and accounts using compromised credentials, particularly where individuals have re-used the same password or a predictable pattern of passwords. This heightens the risk of credential stuffing attacks where credentials obtained from one breach are used to log into an unrelated service.

KEY INSIGHT

Threat actors will combine different pieces of information so reuse of the same password can make accounts easier to be breached.

RECOMMENDATION

Ensure password policies around strength, complexity and auto renew dates are in place, and enable multi-factor authentication on all systems.

HYBRID AND REMOTE WORKING CREATES DIFFERENT RISKS

Working environments have evolved over the last three years, with COVID driving an increase in remote and hybrid work. These changing work environments enable different types of security risks that should be understood.

KEY TAKEAWAY

Consider running an impact assessment starting with the following checklist to help identify and address these risks:

- ☑ How 'security aware' are your employees and contractors? Is training needed to improve capability and understanding?
- ☑ Do your remote working policies and procedures address physical security and access security?
- ☑ Do you understand the risks and benefits of 'bring your own device' (BYOD) for employees?
- ☑ Do you have processes and policies in place to enforce regular password updates, minimum password complexity requirements and mandatory multi-factor authentication for all employees and contractors?

AI IS CHANGING THE GAME

Threat actors are increasing their use of AI which gives them access to sophisticated tools to create new waves of cyber threats. One such tool, 'WormGPT,' a variant of ChatGPT but without its limitations or ethical constraints, is currently available on the dark web.

The use of AI extends beyond conventional hacking by elevating the sophistication of phishing scams. Traditional scams, like poorly written emails from pretend Nigerian princes, are being replaced by impeccably crafted messages that better avoid detection. Social engineering attacks are also increasing as threat actors, leverage AI to create authentic-looking fake accounts for the spread of misinformation.

To combat these challenges defenders can harness AI technologies to identify vulnerabilities and uncover previously unnoticed attacks. This proactive application of AI may ultimately help mitigate the impact on targeted organisations, both in terms of time and financial resources.

KEY TAKEAWAY

AI is changing the game and threat activity is becoming increasingly sophisticated.

★ RECOMMENDATION

Ensure your cyber security applications keep pace and leverage AI for improved threat detection and resolution.

COULD YOUR BUSINESS SURVIVE A BREACH?

The reputational, brand and commercial risk of a breach can't be underestimated. The average cost of a breach for an Australian SMB is estimated at around $25,000, excluding any penalties under the Privacy Act 1988 for serious or repeated privacy breaches. On top of the potential impact of business-critical data being crypto locked and inaccessible for weeks.

Interestingly nearly half of Australians said they would close their account or stop using a product or service provided by an organisation that experienced a data breach. However, most Australians are willing to remain with a breached organisation provided the organisation promptly takes action, such as quickly putting steps in place to prevent customers experiencing further harm from the breach and making improvements to their security practices.

The need for a specific cyber insurance policy is also rising with the increasing threat, costs and penalties.

★ RECOMMENDATIONS

1. We highly recommend all businesses complete a cyber insurance assessment with a qualified insurance or legal advisor to ensure they have adequate coverage in the event of a breach.

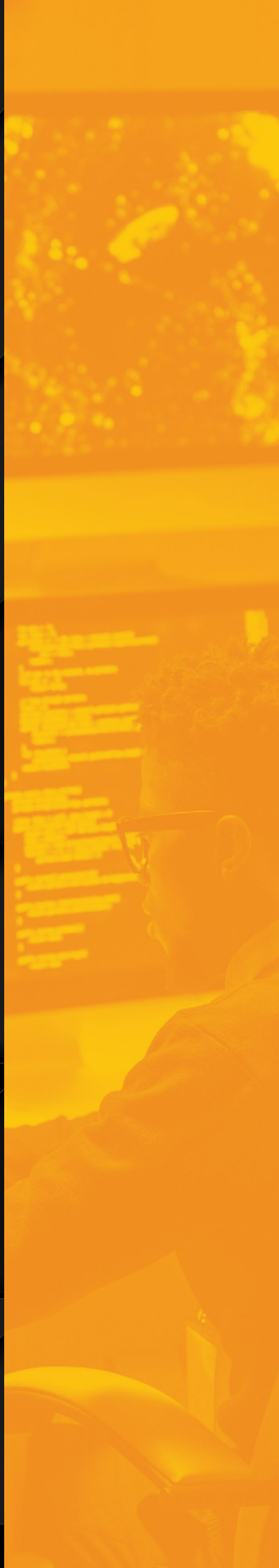
2. Develop a cyber security incident response plan, mapping out the actions to take should you be targeted.

SUMMARY

The threat landscape is changing rapidly, Australian SMBs are seen as easy marks and need to realise that it's only a matter of time before they're targeted. Ensure your bases are covered by obtaining cyber security insurance, define a response plan, establish training, and enable multi-factor authentication on all systems.

Want to know more about the simple steps you can take now to begin reducing your risk? **Talk to us about your cyber assessment today.**

PREMIER
Technology Solutions



About Premier Tech

The Technology Success Partner for progressive businesses that see technology as an enabler for growth.

Premier Tech has redefined what it truly means to support and add value to businesses. In particular, progressive businesses need to strike a balance between responsive, proactive service and strategic thought and care.

Engaging Premier Tech means having us onboard as your Technology Success Partner. We work alongside you to help progress your IT strategy while assisting with day-to-day support to help your business grow and evolve with technology.

Talk to us about your technology needs

1300 767 648
talktous@premiertech.com.au
www.premiertech.com.au