CYBERGUYS

WE'RE TOO SMALL TO BE HACKED:

A DANGEROUS MISCONCEPTION IN THE MODERN ERA

INTRODUCTION

Cybersecurity is a critical concern for all businesses, regardless of size. In recent years, cyberattacks have become more automated, sophisticated, and frequent, affecting companies in every industry.

Unfortunately, many Australian small and medium-sized business owners believe that their businesses are not at risk simply because of their size. This dangerous misconception can lead to costly security breaches and long-lasting consequences.

MYTH:
MOST CYBERATTACKS ARE TARGETED

Much of the industry still views cybercriminals as they are portrayed in movies: expert hackers who carefully choose targets and then work their way through their defences in search of a payday. While this type of cybercriminal certainly does exist, the vast majority are far less sophisticated. Most lack the necessary knowledge and skills to penetrate a specific target's cyber defences, so instead, they look for targets with vulnerabilities they know how to exploit. Because they are picking their targets based on the vulnerabilities they have, not the potential payoff, small businesses often end up in their crosshairs.

Moving even further away from the Hollywood image, most of today's cyberattacks are automated. Cybercriminals use tools to scan the internet for exposed systems and known vulnerabilities. The tools begin the attack, and the human only becomes involved once the exploit has occurred. And automated tools don't care about the size of the business; they just look across the internet for the vulnerabilities they can exploit.

Over the few years, phishing has become an easy way for almost anyone with an internet connection to launch a cyberattack with minimal technical knowledge. Email-based phishing campaigns can be sent to tens of millions of potential victims in a single round. Again, these attacks are not targeted based on the size of the potential payoff but are scattergun-style attacks looking for anyone who misses the warning signs and falls victim. Phishing attacks do not discriminate, and businesses of all sizes fall victim to them every day.

MYTH:
SMALL BUSINESSES ARE NOT TARGETED

When attacks are targeted, far from being deterred by their size, cybercriminals are often attracted to small and medium businesses and actively target them. Because many such businesses operate under the "I'm too small to be hacked" mentality, they can be easier targets for cybercriminals, taking less time, effort and resources to penetrate and ultimately profit from.

Additionally, small and medium-sized businesses are often unaware of the sensitivity of the data they hold and the potential risks they face –meaning that even when they invest in cybersecurity, it can be in the wrong place or leave gaps that expose sensitive data. This makes the data even easier for cybercriminals to steal.

MYTH:
CYBERCRIMINALS ARE LOOKING FOR BIG PAYDAYS

The internet connects nearly 5 billion people around the world. This global reach and accessibility enable cyber attackers to launch their malicious activities from virtually anywhere. Cybercriminals operating from developing nations often seek targets with smaller payout potential, as a relatively small financial reward can yield a disproportionately high purchasing power in such countries. Other cybercriminals may take the view that big paydays that come from big businesses are too complicated or infrequent and actively seek out smaller businesses to achieve smaller but more frequent success in their cyberattacks.

HOW TO PROTECT A SMALL OR MEDIUM-SIZED BUSINESS

A risk-based approach is essential to protect small or medium-sized businesses from increasingly pervasive cyber threats. While these businesses face many of the same cybersecurity risks as larger organisations, they operate with a significantly smaller cybersecurity budget. Because of this, they can often be tempted into simply going out and purchasing a few of the latest cybersecurity products and then calling the problem solved – but such an approach will often lead to a misuse of limited resources and can leave critical areas of vulnerability unprotected.

Instead, a risk-based approach starts with an analysis of the unique risks a business faces and any mitigations already in place. This approach lets businesses prioritise their spending on cybersecurity solutions that address the most significant and likely threats rather than wasting time and money to protect less critical areas.

By identifying and mitigating the most significant risks, businesses can stretch their limited budgets to provide the maximum potential for protection against the most damaging and potentially costly cyber threats.

With a careful analysis of risks and the implementation of targeted solutions, businesses can better protect their assets, customers, and reputation from the most damaging cyberattacks.

A great place to start is the Australian Government's Essential Eight framework. These are the eight cybersecurity areas that the Australian Cyber Security Centre (ACSC) defines as the most important of their wider thirty-seven.

The Essential Eight was designed to provide an easy way for small businesses to begin their cybersecurity journey and to assist all businesses in prioritising their cybersecurity spending. It also provides different levels to which each strategy can be implemented depending on the organisation's specific risks.

CONCLUSION

Being small is no longer a protection against cyberattacks. Cyberattacks have become easier to launch in recent years, less targeted and more automated. This has made cyberattacks more accessible to a broader range of cybercriminals, who are searching for anyone to breach, not just large businesses. 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 conducting a risk-based analysis to understand their own unique set of risks and existing mitigations, and aligning with the Essential Eight framework, small business owners can achieve a high level of protection even working within limited cybersecurity budgets.

Contact Info

07 3326 2373

sales@cyberguys.com.au

www.cyberguys.com.au

CYBERGUYS