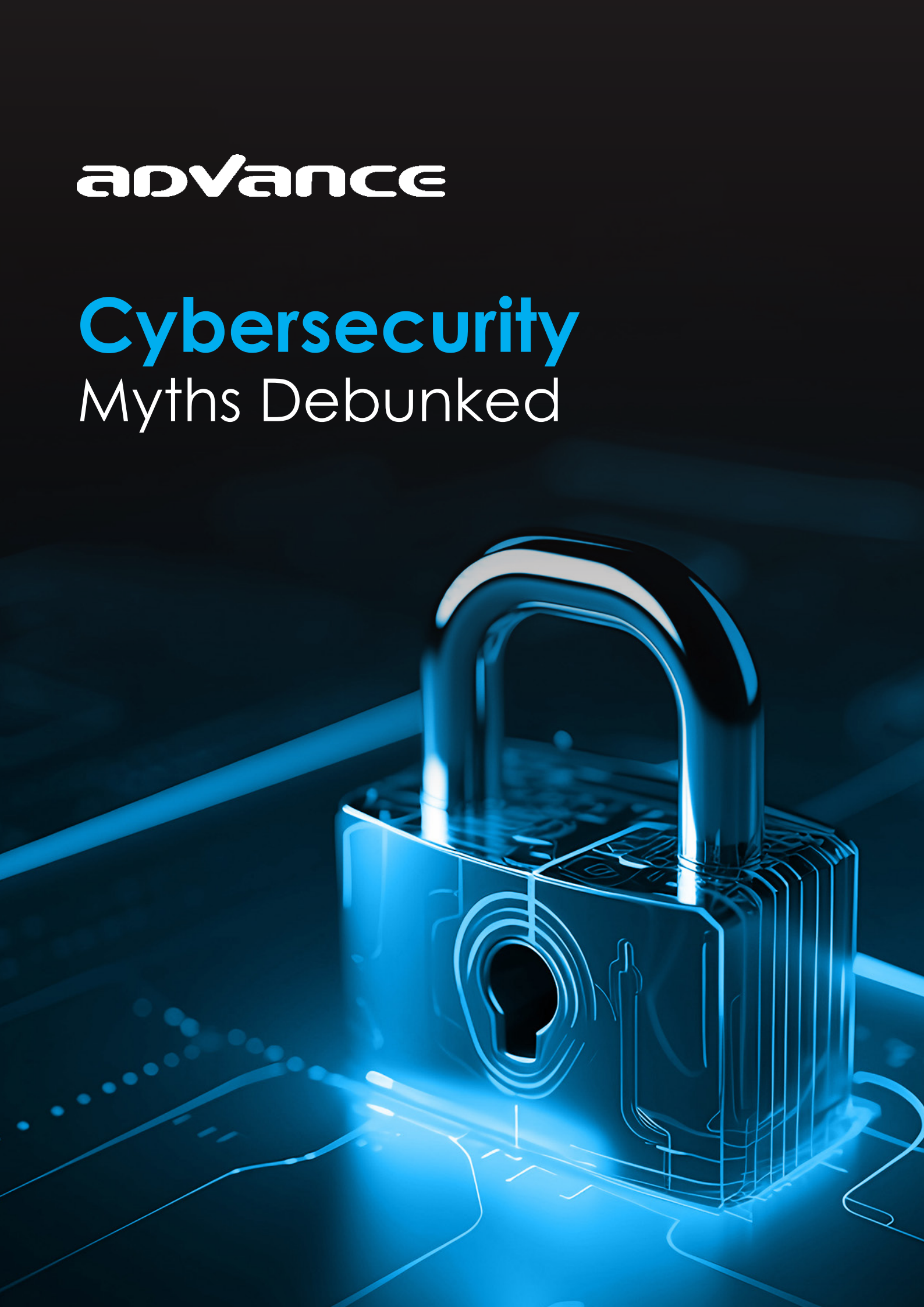
advance

Cybersecurity
Myths Debunked



Introduction

Cybersecurity is no longer a new topic for most organisations. Digital transformation creates incredible opportunities in almost all industries, but it brings with it unique and modern challenges. While those challenges are generally understood, several myths still surround them. In this whitepaper, we take a look at some of the common ones and check the facts.

Common Cybersecurity Myths Expanded

Small Businesses Are Not Targets for Cyberattacks

The prevailing myth that cybercriminals exclusively focus their malicious intentions on large corporations is not only inaccurate but also very deceptive. Cybercriminals rarely select their targets based on perceived size or payday; instead, they look for targets with weaker defences and, therefore, a better chance of 'success' for the cybercriminal.

In fact, it is debatable whether cybercriminals 'target' their attacks. Most attacks start with a scattergun approach, such as sending millions of phishing emails or using automated scanning across the Internet to look for old, known vulnerabilities in connect systems. The attacker only 'targets' an organisation once they know a user is susceptible to phishing or that the organisation has a vulnerability they can exploit.

In addressing this myth, it's crucial to understand that cybersecurity is an omnipresent threat, not a hypothetical risk. The question is not if an SME will face a cyberattack but when. Therefore, businesses of all sizes, irrespective of their market footprint or industry, must adopt a proactive stance towards cybersecurity. This involves not only recognising the risks but also implementing comprehensive security strategies to mitigate them.

A Basic Antivirus Is Sufficient for Protection

The second myth revolves around the adequacy of antivirus software in the grand scheme of cybersecurity. While it's indisputable that antivirus programs constitute a fundamental component of a robust digital defence, over-reliance on them is a miscalculation. The cyber threat landscape has undergone a significant transformation, becoming increasingly sophisticated and complex. Modern cyber threats can easily circumvent the defences of basic antivirus solutions, exploiting vulnerabilities beyond their scope of detection and prevention.

To effectively counteract these advanced threats, a layered security approach is imperative. This strategy involves employing multiple layers of defence, each designed to protect against different types of cyber threats. These can include firewalls, intrusion detection systems, regular software updates, employee cybersecurity training, and more. By layering these defences, an organisation can ensure that if one layer is compromised, others are in place to stop an attack.

Cybersecurity Is Solely a Tech Department Concern

The next myth to dispel is the notion that cybersecurity concerns are confined to the IT or tech department. This outdated perspective fails to recognise cybersecurity as a pervasive business issue that impacts every facet of an organisation. In the digital era, every employee, from the executive suite to entry-level interns, plays a crucial role in maintaining and enhancing the organisation's security posture.

Cybersecurity awareness and protocols must be ingrained in the company culture, transcending departmental boundaries. Regular training sessions, clear communication of security policies, and fostering a culture of vigilance and responsibility are critical steps in this direction. By involving all employees in cybersecurity efforts, an organisation builds a robust, company-wide defence against potential cyber threats.

Strong Passwords Are Enough to Keep Data Safe

The belief that robust passwords alone are the cornerstone of data security is a common misconception. While a strong password is undoubtedly a fundamental aspect of safeguarding digital information, it's far from a foolproof defence mechanism. In the sophisticated arena of cybercrime, hackers employ a variety of techniques to undermine password security. These techniques include, but are not limited to, phishing attacks, where unsuspecting users are tricked into revealing their passwords; keylogging, where malicious software records every keystroke, capturing passwords as they are typed; and credential stuffing, where the username and password combinations are stolen from one system, and used to log into another.

Modern digital security demands more robust measures, such as Multi-factor Authentication (MFA). MFA enhances security by requiring multiple forms of verification before granting access. This might include something the user knows (like a password), something the user has (like a mobile device), and something the user is (like a fingerprint or facial recognition). By integrating MFA into security protocols, the likelihood of unauthorised access is substantially reduced, as it becomes significantly more challenging for cybercriminals to bypass multiple security layers.

Cyber Attacks Are Always Obvious

Many business owners and managers believe that cyber-attacks are immediately noticeable. However, the reality is that cyber-attacks can be exceedingly stealthy and sophisticated. Advanced Persistent Threats (APTs) exemplify this stealthiness. APTs are prolonged and targeted cyberattacks wherein an unauthorised user gains access to a network and remains undetected for an extended period. During this time, they can continuously steal sensitive data, causing substantial damage without any immediate signs of their presence.

Regular system audits are essential to counter these insidious threats. These audits should comprehensively examine and assess the integrity of the digital infrastructure, seeking any anomalies or breaches that might indicate a security compromise. Additionally, fostering a culture of vigilance among employees is crucial. Staff should be trained to recognise and report unusual system behaviour, which could be indicative of a cyber intrusion.

Cybersecurity Insurance Is Unnecessary If You Have Good Security Controls

Another myth to debunk is the notion that robust security measures negate the need for cybersecurity insurance. While implementing strong security controls is undoubtedly critical, it's also important to recognise that no system is completely invulnerable. Cybersecurity insurance acts as a vital safety net, providing a layer of financial protection in the event of a security breach.

This type of insurance can be particularly vital for SMEs, as the financial implications of a cyberattack can be devastating. Cybersecurity insurance policies typically cover various expenses, including legal fees, fines, and the costs associated with data recovery and system repairs. Additionally, they might also cover the expenses related to notifying customers of a breach and managing public relations fallout. By having cybersecurity insurance, SMEs can ensure that they have the necessary resources to recover and continue operations following a cyber incident, safeguarding their long-term viability.

Patching Software Is a Low-Priority Task

The misconception that updating and patching software is a task of low importance can significantly jeopardise an organisation's security. Software updates are far more than just performance enhancements or new features; they are critical for plugging security vulnerabilities. When software companies discover vulnerabilities in their products, they issue patches to rectify these flaws. Delaying these updates leaves systems susceptible to known exploits, which cybercriminals are constantly on the lookout to exploit.

Regular and efficient patch management is a crucial security practice. This involves not just the occasional updating of systems but a structured process where all software used by an organisation is consistently monitored and updated to its latest version. This proactive approach ensures that any potential vulnerabilities are addressed promptly, thereby fortifying the organisation's defences against potential cyberattacks.

Once a System Is Secure, It's Secure Indefinitely

Many assume that once they have set up a robust cybersecurity system, it will remain effective indefinitely. This is far from the truth. The realm of cybersecurity is dynamic, with threats evolving at a rapid pace. What is deemed secure today might be vulnerable tomorrow.

Ongoing vigilance is essential. This includes continuous monitoring of systems, regular updates to security practices, and consistent employee training to adapt to the changing threat landscape. Cybersecurity is not a static setup; it's an evolving process that requires regular reassessment and adaptation.

Cybersecurity Insurance Is the Only Defence You Need

Finally, there is a growing reliance on cybersecurity insurance as a sole line of defence. While cybersecurity insurance is a vital component of a comprehensive security strategy, it is not a standalone solution. Relying exclusively on cyber insurance is akin to having home and contents insurance and leaving all the doors unlocked.

Cybersecurity insurance is designed to mitigate the financial impact of a cyber incident, but it does not prevent the incident from occurring. Proactive security measures, including risk assessments, security protocols, and preventive technologies, are essential to thwart cyber threats before they materialise.

Conclusion

The digital landscape is fraught with misconceptions that can lead organisations to make misguided decisions about their cybersecurity. By debunking the common myths surrounding cybersecurity, it becomes evident that a proactive, informed, and layered approach to digital defence is not just recommended, it is essential for the survival and prosperity of any business in today's interconnected world.

Cybersecurity is not a static entity but a dynamic and ongoing process that adapts to new threats as they arise. It requires constant vigilance, a culture of security awareness, and the implementation of strategic defences that protect against a multitude of potential attacks. For SMEs, the investment in robust cybersecurity measures is not a luxury; it is a fundamental aspect of operating in the modern business environment.

The steps outlined in this article are not exhaustive but serve as a foundational guide for organisations to better understand the risks they face. Regular reviews and updates to practices, in conjunction with staying abreast of the latest cybersecurity trends and threats, will further reinforce an organisation's defence mechanisms.

As the digital age progresses, the commitment to cybersecurity must evolve in tandem. The measures an organisation takes today will define its resilience against the cyber threats of tomorrow.

Contact info

+61 8 8238 6500

sales@advance.net.au

www.advance.net.au