Cyber 101: how your business is at risk

Cybersecurity threats you can't afford to ignore

A lot of organisations believe they're too small to be targeted – that it isn't worth hackers' time and effort to go after them – or assume that their IT provider already has everything covered. In fact, SMEs are among the most vulnerable targets, and most breaches exploit basic, avoidable gaps.

Here are the most common weaknesses we encounter here at Sentis.

Phishing and social engineering

Phishing tactics are more sophisticated than ever, with tailored messages, fake invoices, impersonations of suppliers and even AI-generated content. One click from a poorly trained employee can expose credentials, financial data and customer information.

This is why regular staff training is key – because when it comes to cybersecurity, your workforce is your business's first line of defence.

Ransomware and data extortion

Modern ransomware doesn't just lock you out of files; first, it steals your data. Even if you can restore from backup, leaks of customer or employee data can do lasting damage to your reputation – as well as hitting your business in the pocket.

Without strong endpoint protection, system monitoring and battle-ready recovery plans, being hit by ransomware can also cause significant disruption.

Supply chain risk

Your security is only as strong as that of your suppliers and partners. If a third party is compromised, attackers can exploit that trust relationship to access your systems or data.

Without adequate controls and detailed due diligence, supply chains remain a major source of cybersecurity risk.

Stolen credentials

Attackers can crack weak passwords and reused logins, allowing them to quietly work their way through your emails, finance platforms and cloud-based systems. Sometimes they can go undetected for weeks.

Unless you've enabled multi-factor authentication and hold regular reviews of who has access to what, your systems are like an open goal for online criminals.

Patch management gaps

Cyber criminals seize on known vulnerabilities. If software updates and security patches aren't applied promptly and consistently, you're leaving your business vulnerable to attack – often involving issues for which there's already a fix available.

No standards, poor governance

In the absence of recognised cybersecurity standards like Cyber Essentials, plus clear policies and robust oversight, security is reactive and after-the-fact, not proactive and strategic. This lack of structure provides attackers with a wealth of opportunities they won't hesitate to exploit.

Cyber risk doesn't have to be overwhelming, but it won't simply disappear if you ignore it. So, if you're not sure where your vulnerabilities lie, you need to find out without further delay.

Sentis Managed Solutions can help your business protect itself against cyber threats using cutting-edge tech, as well as staff training by our experts.

Visit our website at sentisms.com for more.