RISKY BUSINESS

James Griffin *reveals why the UK's new cyber law makes relying only on Microsoft 365 security a risky move for MSPs*

The UK's Cyber Security and Resilience Bill will demand a rethink among Managed Service Providers (MSPs). With the UK Parliament set to grant regulators more teeth, MSPs will face tougher expectations not just around best practice, but mandatory compliance. The Bill is anticipated to reach Parliament in the second half of 2025, although the exact timeline remains uncertain. One thing is clear: relying solely on native Microsoft 365 security features will not be good enough.

Despite what the E5 licence price tag might suggest, Microsoft's native tools – Exchange Online Protection, Defender for Office 365 and Purview – leave dangerous blind spots such as gaps in detection and response, configuration complexity and inconsistency and the risk of single-vendor reliance. The government knows it, threat actors know it and if MSPs don't get ahead of it, their clients will soon find out the hard way.

Relying solely on Microsoft 365 for security leaves MSPs exposed to growing threats like BEC attacks, phishing and QR code scams. With the UK's Cyber Security and Resilience Bill set to raise the bar on compliance and reporting, MSPs must move beyond native tools and adopt a layered security strategy to demonstrate true operational resilience.

THE REALITY OF SHARED RESPONSIBILITY

Microsoft operates under a shared responsibility model, meaning it keeps the cloud infrastructure running, but the responsibility for protecting the data is on the customer. Or, in the case of most UK SMBs, on the MSP they work with. This is where the cracks can start to show. Exchange Online Protection misses low-volume Business Email Compromise (BEC) attacks. Defender isn't tuned for QR code phishing or MFA bypasses. Audit logs? They're either buried in Purview or missing altogether on lower-tier plans.

We all know that the threat of a breach is real and growing. Indeed, our own recent research confirms this and paints quite a stark picture:

- 64 percent of organisations expected phishing threats to increase in 2025.
- 1 in 5 MSP customers suffered a successful BEC attack in 2024.
- 45 percent of MSP customers experienced a breach of sensitive employee data.
- Over 20 percent were hit by credential theft via QR code phishing, an attack vector that bypassed Microsoft 365's native defences entirely.

Take the increasing use of generative AI and deepfake-based impersonation attacks into account, and the potential risk grows exponentially. These aren't theoretical threats; they're happening now – and the regulators are watching.

I'm not calling for you to abandon Microsoft and its native security tools, but there needs to be a sense of realism. Microsoft 365 is a powerful productivity suite, but it's not a fully-fledged cyber security platform. In fact, 98 percent of the organisations sampled in our research using Microsoft 365 said that third-party security solutions are: "highly important" for defending against advanced threats.

Microsoft 365 is a powerful productivity suite, but it's not a fully-fledged cyber security platform

Perhaps this is why MSPs are shifting to layered protection strategies such as:

- AI-powered email filtering and behavioural detection
- DNS-level filtering and link rewriting
- Proactive phishing simulation and user training
- Backup and rapid recovery across email, endpoints and SaaS apps

This isn't security overkill; it's the modern-day baseline.

GET AHEAD OF THE GAME

The upcoming Cyber Security and Resilience Bill aims to drive up standards and is expected to introduce stricter incident reporting obligations, resilience testing and penalties for non-compliance. Smart MSPs are taking the opportunity to reassess their tech stack. This isn't only for the sake of compliance, but also because the reputational and financial damage from a breach is too great to risk. MSPs must demonstrate not only uptime, but also proactive cyber resilience – the ability to detect, defend, respond and recover at speed.

If you're an MSP relying solely on Microsoft 365 to keep clients safe, you're not just under-protected – you're under prepared. The cyber security landscape has changed, the law is catching up, and it's time your security strategy changed too ●

James Griffin is CEO at CyberSentriq.