Cyber Security Matters Now

+16% growth in UK "serious" cyber incidents from 2023 to 2024

77% of UK firms will increase their cyber security spend in 2025

43%
of UK businesses experienced a cyber breach or attack in the last 12 months

84%
of businesses reported breaches or attacks that included phishing attempts

£3.4bn
estimated annual cost to UK SMEs from cyber-hackers

60%
cite "increasing sophistication of threats" as a top concern

52%
of SME employees have never had cyber security training

32%
of UK SMEs have no cyber security protections at all

- **Phishing and Malware remain entry-points** for most breaches. Even simple attacks can lead to big damage if defences are weak. Antivirus, email filtering and staff awareness are **must haves**, not optional
- **Ransomware is rising, both in frequency and sophistication** (double extortion) which means businesses with weak backups, weak internal segmentation (Zero Trust, remote access, firewalls, etc.) stand to lose more
- **Costs per incident are rising for SMEs**, and it's not just the cost of the ransom that's needed to be considered, it's the **cost of downtime, customer churn and reputational loss** too
- **Many SMEs are under-prepared** to deal with a cyber attack; lacking incident plans, risk assessments and training - even basic protections. **This gap is exactly where a layered, fully-stack defence can make the difference**
- **Remote working and supply chain vulnerabilities** widen the attack surface. With employees working offsite or using own devices, the risk of remote access exploitation or third-party risk is higher now than ever