FMBusinessDaily

Nearly 1 in 4 UK SMEs identify remote working as a key cybersecurity concern, new study reveals

10 months ago

A new study by Markel Direct, the specialist insurer of small businesses, has revealed that nearly 1 in 4 SMEs are concerned about how they secure remote working environments for employees working away from the office.

The survey, which asked 500 SME owners to share the challenges they are facing when it comes to cyber security, identified that securing remote working environments was a key concern for 23% of SMEs. It ranked in second place in the list of cyber security concerns for the future for SMEs, with the increased sophistication of cyber threats firmly in the top spot with an overwhelming 62% of respondents reporting it as a concern.

When asked how those with remote workers ensure the security of company data when accessed by employees working from home, the majority (52%) said they use virtual private network (VPN) access, 48% train their employees on secure remote work practices and 46% have remote access policies and controls in place.

Nearly half of SMEs don’t know what to do in the event of a cyber attack

The study also found that 49% of SMEs wouldn’t know what to do in the event of their business suffering a cyber-attack, and 69% didn’t have a cyber security policy in place.

Despite this, most UK SMEs are taking some proactive measures to prevent cyber-attacks, with 72% having invested in antivirus/anti-malware software. Nearly seven in ten make sure they regularly update their system software (69%) and 52% are making use of multi-factor authentication.

How UK SMEs are facing up to cyber threats

Measures in place to prevent cyber attacks	% of SMEs with these in place
Have antivirus/anti-malware software	72%
Regularly update system software	69%
Keep IT systems up to date	53%
Use multi-factor or two-factor authentication	52%
Email filtering for spam and phishing emails	49%
Staff training	49%
Have a firewall	47%
Secure Wi-Fi networks	46%
Conduct regular data backups	46%
Data encryption	44%
Encourage employees to update passwords	35%

However, there is more that could be done, as 43% said that their employees are not trained on best practices and potential threats, and over half (53%) do not have cyber insurance in place in case of a breach, leaving their businesses vulnerable.

Rob Rees, Divisional Director of Markel Direct, said ‘Staying ahead of cyber threats is crucial for small business owners, especially as AI-driven attacks continue to evolve. Having a robust cyber security policy in place can help create a framework to safeguard against ongoing threats, whilst cyber insurance can help to protect your business in the event of a targeted attack.

“Almost half of SMEs reported not knowing what to do in the event of a cyber-attack – something that can be key to mitigating its impact. This is why we provide Markel Direct cyber insurance policyholders with access to a cyber response helpline; so that expert guidance is on hand to help small business owners should they experience a cyber security incident.”

You can find the full study here: https://www.markeluk.com/cyberscape