50% of businesses say they have experienced a cyber attack in the last 12 months.

But this rises to 58% for small businesses and 70% for medium businesses. SMBs like yours may not have in-house tech experts or the budget to employ full-time specialists, but here are 10 common cyber security blind spots that you shouldn't overlook.

1 Outdated Software and Systems:

When you're hands-on with multiple aspects of the business, regular updates to software and systems can get pushed to the bottom of the list. This can leave you open to attack from hackers who target known vulnerabilities in outdated applications or operating systems.

Solution: Use tools to check for and apply automatic updates; implement policies to carry out regular updates; have experts assess your estate for vulnerabilities.

2 Lack of Employee Training:

Without proper training, employees can create vulnerabilities in a business's cyber security. They may unintentionally fall victim to phishing attacks, use weak passwords, or inadvertently download malware.

Solution: Carry out regular training so colleagues understand and recognise the latest threats and scams; deliver refresher courses to make sure they know the role they play in maintaining security.

3 Weak Password Practices:

Weak and reused passwords can be easily compromised, leaving sensitive data vulnerable to cybercriminals. It might sound obvious, but in 2023, more than a fifth of web application attacks were caused by easily guessed passwords. Don't add your business to that list.

Solution: Encourage and enforce strong password policies, using combinations of upper case letters, lower case letters, numbers and symbols.
Change passwords regularly.

4 Unsecured Wi-Fi Networks:

Using default settings or weak encryption on Wi-Fi networks can allow attackers to gain unauthorised access to your internal network. This can make it vulnerable to a range of threats including malware, phishing, ransomware or even DDoS attacks which can force your service offline.

Solution: Adopt security controls like firewalls, intrusion detection and network access controls, that spot and prevent unwanted visitors to your network. Encrypt data so that it can't be intercepted or stolen.

5 Third-Party Vendor Risk:

Most businesses outsource at least part of their businesses – and these external vendors may not have strong security practices. A breach in a vendor's system could lead to a breach in yours, which could affect your operations and put your reputation at risk.

Solution: Evaluate the security of every member of your digital supply chain to make sure you have the same attitude to cyber threats and the levels of protection you need.

6 Insufficient Data Backup:

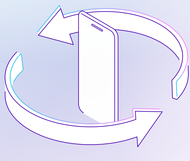
It's estimated that almost half of small businesses lack the backup measures to prevent catastrophic data loss. Without a regular, secure, backup of your data, you leave yourself open to ransomware attacks or other cyber threats.

Solution: Safeguard your business data with encrypted cloud backup. Stored remotely for easy and cost-efficient access, your data is inaccessible and unreadable to would-be cyber criminals and all is not lost if the worst happens.

7 Inadequate Access Controls:

Without proper access controls, unauthorised people can get hold of your sensitive data and get into your systems – whether by accident or with cyber crime in mind.

Solution: Put strict access and authentication controls in place to make sure only the people who are authorised can access your business systems and data.



8 Neglecting Mobile Device Security:

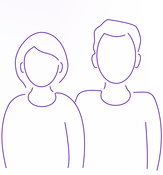
It's easy to overlook the network entry points that your employees carry round with them. But if your people are using their personal or company mobile phones for work, then they're vulnerable to cyber threats.

Solution: Consider mobile-specific security solutions to secure your mobile devices, intercept cyber attacks and keep your business safer, no matter where your people are working.

9 Ignoring Incident Response Planning:

Hope for the best, prepare for the worst. Without an incident response plan, it's almost impossible to control the effects of a data breach.

Solution: Develop a detailed plan that includes processes, roles, responsibilities and communication guidelines if a security breach takes place. Backing up your data will help too!



10 Underestimating Insider Threats:

They might not mean to, but people working inside your business can pose a threat to your security too. If you're not monitoring or controlling your network, then you might not notice when someone's doing something they shouldn't.

Solution: Consider network monitoring tools to keep an eye on network traffic and flag up any suspicious activity. Allowing you to take action before it becomes a more serious problem.

To remove your blind spots, search BT Cyber Security.