Cybersecurity Checklist for Small Businesses

Use this checklist to ensure your small business is protected against common cyber threats and compliant with key regulations in 2025.

1. Assess Your Cybersecurity Posture

☐ Conduct a risk assessment to identify potential vulnerabilities.
☐ Map critical assets, including customer data, intellectual property, and financial records.
☐ Perform penetration testing to uncover hidden weaknesses in your system (3rd party services can help with this).

2. Implement Essential Security Measures

☐ Update all software and systems regularly to apply security patches.
☐ Enforce multi-factor authentication (MFA) for all employees and accounts.
☐ Use strong password policies requiring at least 12 characters and promote the use of password managers.
☐ Encrypt sensitive data at rest and in transit, including emails and customer information.
☐ Regularly back up data to secure, offsite locations and test backups for reliability.

3. Strengthen Defences

☐ Install and maintain firewalls and endpoint security solutions.
☐ Use AI-powered threat detection tools to monitor network activity for unusual behaviour.
☐ Adopt a zero-trust security model by verifying every access attempt, even within your network.

4. Build Employee Awareness

☐ Provide at least quarterly cybersecurity training to help employees recognise phishing attempts and other scams.
☐ Gamify training to increase engagement and knowledge retention.
☐ Establish clear reporting procedures for suspicious activity.

5. Evaluate Third-Party and Cloud Security

☐ Assess the cybersecurity policies of all vendors and third-party services.
☐ Review cloud configuration settings to prevent misconfigurations.
☐ Use cloud security platforms like AWS Shield or Microsoft Defender and Azure Security Centre.

6. Develop Cybersecurity Processes

☐ Create a detailed incident response plan with clear steps for handling breaches.
☐ Schedule regular security audits to review your IT infrastructure and policies.
☐ Define and enforce access control policies, limiting employee access to only the data they need.

7. Stay Compliant with Regulations

☐ Review and comply with relevant data protection laws like GDPR, UK Data Protection Act and sector specific regulations.
☐ Keep detailed records of cybersecurity policies and compliance activities.
☐ Work with legal or IT consultants to prepare for audits and regulatory updates.

8. Protect Your Business Financially

☐ Obtain cyber insurance to cover data breaches, legal expenses, and business interruptions.
☐ Ensure your insurance policy includes coverage for ransomware and data recovery costs.

9. Monitor and Measure Progress

☐ Set and track key performance indicators (KPIs), such as time to detect and respond to incidents.
☐ Use dashboards to visualize your security posture and make informed decisions.
☐ Conduct regular phishing simulations and track employee performance in training.

Final Review

☐ Are all systems up to date and secure?
☐ Do employees understand their roles in maintaining cybersecurity?
☐ Have you tested your incident response and recovery plans?

By following this checklist, your small business can reduce vulnerabilities, protect sensitive information, and build resilience against the evolving cyber threats of 2025 and beyond.