Cyber Insurance Readiness Checklist for Small Businesses (2026 Edition)

Use this checklist to see whether your business is ready before you apply, renew, or answer underwriting questions.

Cyber Insurance Readiness Checklist

1. Multi-Factor Authentication Is Enforced

□ MFA is enabled for email, remote access, admin accounts, and critical apps
□ MFA is required for all users, not just optional for some
□ Stronger methods are used where possible instead of SMS alone

Why this matters:
MFA remains one of the most common controls insurers expect to see, especially for internet-facing and privileged accounts. CISA and insurer guidance continue to treat it as foundational.

2. Endpoint Protection and Detection Are Active

□ Company devices have antivirus or EDR in place
□ Alerts are monitored and reviewed
□ Unmanaged devices are identified and addressed

Why this matters:
Traditional antivirus alone is often treated as insufficient for modern threats. Current insurer-facing guidance increasingly points to endpoint detection and response as an important control.

3. Backups Are Isolated, Tested, and Recoverable

□ Backups run on a regular schedule
□ At least one backup copy is stored separately from the main network
□ Restore testing has been performed recently
□ Backup failures are reviewed and fixed

Why this matters:
Insurers and CISA both emphasize that good backups must be more than "configured." They need separation from production systems and regular restore testing.

4. Patch and Update Management Is Consistent

□ Operating systems are updated regularly
□ Critical software and internet-facing systems are patched promptly
□ Unsupported software is identified and replaced

Why this matters:
Insurers and security guidance repeatedly highlight outdated systems as avoidable risk. Regular patching remains one of the clearest underwriting and security readiness signals.

5. Access Is Controlled by Role

□ Employees only have access to what they need
□ Admin rights are limited
□ Former users and stale accounts are removed promptly
□ Shared accounts are minimized and reviewed

Why this matters:
Identity and access management, least privilege, and data access controls are common expectations in both insurer and security framework guidance.

6. Passwords and Credential Management Are Under Control

□ A password manager is in use for business credentials
□ Reused or weak passwords have been eliminated
□ Shared credentials are stored securely, not in email or spreadsheets
□ Privileged credentials are reviewed separately

Why this matters:
Strong password controls and credential hygiene still matter, especially because credential abuse is central to many claims scenarios involving email compromise and ransomware.

7. Employees Receive Security Awareness Training

□ Employees receive phishing and cyber awareness training
□ New hires are trained early
□ Suspicious emails or login prompts are reported through a clear process

Why this matters:
Training remains one of the most frequently cited insurer requirements because human error and phishing continue to drive incidents.

8. Incident Response Planning Exists

□ A basic incident response plan is written down
□ Key contacts are documented
□ The business knows who handles communications, IT response, and escalation
□ The plan is reviewed or exercised periodically

Why this matters:
CISA explicitly recommends maintaining and exercising an incident response plan, and insurers increasingly view response readiness as part of overall cyber maturity.

9. Email Security and Business Email Compromise Controls Are in Place

□ Email filtering is active
□ Suspicious messages can be reported easily
□ High-risk payment or vendor-change emails are verified through another channel
□ Mailbox forwarding rules are reviewed

Why this matters:
Business email compromise remains one of the biggest practical loss areas for businesses, and insurers increasingly look at controls around email and payment fraud exposure.

10. Funds Transfer and Approval Controls Are Documented

□ Wire transfers require secondary approval
□ Vendor payment changes are verified outside email
□ High-risk financial actions are not handled by one person alone

Why this matters:
Dual approval and verification controls are increasingly relevant in underwriting because social engineering and payment fraud claims remain costly.

11. Remote Access Is Secured

□ VPN, remote desktop, or other remote tools are protected with MFA
□ Unused remote access tools are disabled
□ Remote access is limited to those who actually need it

Why this matters:
Remote access remains a major risk area in ransomware and insurer guidance, especially when exposed systems lack strong authentication and monitoring.

12. Documentation for the Insurance Application Is Ready

☐ You can answer questions about MFA truthfully
☐ You know what backup system you use and when it was last tested
☐ You can identify your endpoint protection tools
☐ You know whether you have an IR plan and employee training process
☐ Your IT provider can help validate technical answers before submission

Why this matters:
Accuracy on the application matters. Insurer-side guidance stresses helping applicants answer technical questions correctly and involving IT support where needed.

What To Review Before Applying or Renewing

- **MFA coverage**
- **Backup testing records**
- **Endpoint protection status**
- **Incident response contact list**
- **Employee training records**
- **Payment approval procedures**

Why this matters:
These are the areas most likely to expose a weak answer during underwriting or renewal review. They also map directly to practical breach risk.

Quick Rule of Thumb

Cyber insurance readiness is not just:
“Do we have a policy?”

It is:
“Can we prove we have the controls insurers expect before something goes wrong?”