



Cyber Insurance Readiness Checklist

A business-friendly checklist to prepare for cyber insurance questionnaires and renewal reviews.

Your IT Department. Your Cybersecurity Team. Your Technology Partner.

Network Solutionist, LLC

Serving Wilmington, Newark, Middletown, Dover, Rehoboth Beach, and businesses across Delaware.



Why Preparation Matters

Cyber insurance applications increasingly ask about MFA, backups, endpoint protection, employee training, patching, incident response, and vendor access. Having documentation ready can make the renewal process smoother and reduce surprises.

Readiness Checklist

Done	Security Item	Why It Matters
☐	MFA is enforced for email, remote access, administrator access, and critical applications.	MFA is one of the most common insurance questionnaire topics.
☐	Endpoint protection is deployed to all workstations and servers.	Carriers often ask how malware and suspicious activity are detected.
☐	Backups are performed regularly and restore tests are documented.	Proof of recoverability is important after ransomware events.
☐	Security awareness training and phishing education are documented.	Employee training shows an active risk reduction program.
☐	Patch management process is documented.	Insurers may ask how quickly vulnerabilities are addressed.
☐	Incident response plan exists and includes contact details.	A plan helps leadership respond quickly and consistently.
☐	Admin access is limited and reviewed.	Privileged access should be controlled and auditable.
☐	Vendor remote access is documented and secured.	Third-party access is a common source of risk.
☐	Email authentication controls are configured.	SPF, DKIM, and DMARC support anti-spoofing strategy.
☐	Security policies are reviewed at least annually.	Policies should reflect current technology and business practices.

Documents to Keep Ready

- Network diagram or system inventory.
- Backup schedule and latest restore test results.
- MFA enforcement evidence or screenshots.
- Endpoint protection dashboard summary.



-
- Incident response plan and escalation contacts.
 - Employee training records.
 - List of critical vendors and remote access methods.

Helpful Reference Points

- FTC cybersecurity guidance includes cyber insurance as a topic for small businesses and emphasizes protecting data, MFA, backups, and security practices.
- CISA resources for small and medium-sized businesses include materials on phishing, passwords, MFA, software updates, logging, backups, and encryption.

Disclaimer

This guide is for general educational purposes and does not replace a formal cybersecurity assessment, compliance review, or incident response engagement.

Need help turning this into an action plan?

Network Solutionist, LLC can help assess, secure, monitor, and support your business technology environment. (302) 485-9850 | info@nsolutionist.com | nsolutionist.com

