Cyber Insurance Requirements Checklist

What carriers actually require to write or renew a policy in 2026

Cyber insurance underwriting standards have tightened sharply since 2022. Most carriers now decline policies — or refuse to renew — when basic security controls are missing. Use this checklist to gauge your readiness *before* your renewal application lands on an underwriter's desk. **Click each box that applies to your business** — this PDF is interactive.

IDENTITY & ACCESS

- ☐ Multi-factor authentication (MFA) is enabled for ALL administrative and privileged accounts.
- ☐ MFA is required for all remote access — VPN, RDP, cloud admin portals, M365 / Google Workspace admin consoles.
- ☐ Inactive user accounts are disabled or removed within 30 days of employee departure.
- ☐ Users do **not** have local administrator rights on their daily-use devices.
- ☐ Password policy enforces 12+ characters (or passphrase format) with a tested credential manager available.

ENDPOINT SECURITY

- ☐ Endpoint Detection and Response (EDR) is deployed on every workstation and server — not just legacy antivirus.
- ☐ All endpoints receive OS and application security patches within 30 days of release.
- ☐ Office macros are disabled or restricted by default, especially on files from the internet.
- ☐ Mobile devices accessing company data are enrolled in MDM (Mobile Device Management).

EMAIL SECURITY

- ☐ Advanced email filtering (beyond basic spam) is active — phishing detection, attachment sandboxing, link rewriting.
- ☐ Email anti-spoofing protections (SPF, DKIM, DMARC) are properly configured for your domain.
- ☐ External email warning banners are visible on messages originating outside your organization.

BACKUP & RECOVERY

- ☐ Backups run automatically on a regular schedule — at minimum daily for critical data.
- ☐ At least one backup copy is offsite OR stored in immutable format that ransomware cannot encrypt.
- ☐ Full backup restoration is tested at least annually — not just file-level checks, an actual restore.
- ☐ Backup access requires separate credentials from production system access (no shared admin accounts).

TRAINING & AWARENESS

- ☐ All employees complete security awareness training at least annually.
- ☐ Phishing simulations are run at least quarterly (some carriers now require monthly).
- ☐ New hires complete security training within their first 30 days of employment.

NETWORK & INFRASTRUCTURE

- ☐ Critical systems (servers, finance, HR data) are network-segmented from general user traffic.
- ☐ A modern firewall with active intrusion prevention is in place at every network edge.
- ☐ DNS or web filtering blocks access to known malicious sites at the network level.

INCIDENT RESPONSE

- ☐ A written Incident Response Plan exists and identifies exactly who to call when something happens.
- ☐ The IR plan has been tested via tabletop exercise at least once in the past 12 months.
- ☐ Cyber insurance carrier contact information is documented and accessible *offline* (not just in email).

DOCUMENTATION & GOVERNANCE

- ☐ An inventory of all hardware, software, and cloud services is maintained and current.
- ☐ Vendor and third-party risk is assessed before granting access to your systems or data.
- ☐ Security policies (acceptable use, password, BYOD) are documented and formally acknowledged by employees.

How to Read Your Score

25–28 checked	**Strong posture.** Your carrier should write or renew without friction. Most insurers will offer favorable rates at this level.
18–24 checked	**Likely to qualify, with conditions.** Expect higher premiums or requirements to remediate gaps before binding. Address weak areas before renewal.
11–17 checked	**Significant exposure.** Many carriers will decline or require remediation before issuing a policy. Premium will be materially higher.
0–10 checked	**Most carriers will decline.** Treat this as urgent. Your exposure to ransomware, business email compromise, and data breach is severe.

Your Score

Click checkboxes above to calculate your score

Ready to Send Your Results?

Once you've checked the boxes that apply to your business, **save this filled PDF** (File → Save As), then click the button below to email it to us. We'll review your results at no charge and follow up with what we'd prioritize for your environment.

EMAIL YOUR COMPLETED CHECKLIST

*Or attach this PDF to an email manually and send to **GetInfoQuickly@TrinitySolutionsInc.com***

Acronyms Used in This Checklist

MFA **Multi-Factor Authentication — proves identity with more than one factor.**	**EDR** **Endpoint Detection and Response — modern replacement for antivirus.**
MDM **Mobile Device Management — security controls for phones and tablets.**	**RDP** **Remote Desktop Protocol — for connecting to a remote computer.**
VPN **Virtual Private Network — encrypted tunnel into a private network.**	**BYOD** **Bring Your Own Device — employees using personal devices for work.**
SPF / DKIM / DMARC **Email authentication standards that prevent spoofing.**	**IR Plan** **Incident Response Plan — documented playbook for cyber events.**
Immutable Backup **A backup that cannot be altered or encrypted after writing.**	**Network Segmentation** **Splitting your network so a breach in one area can't spread.**

*For full plain-English definitions, see our **Cybersecurity Glossary** at trinitysolutionsinc.com/cybersecurity-glossary/*

Need Help Closing the Gaps?

Trinity Solutions has helped 200+ Triad organizations meet cyber insurance requirements since 2018, with zero successful cyber events on our managed clients.

336-303-1730 | TrinitySolutionsInc.com/Contact-us/