Cyber Insurance Requirements Checklist

A Practical Guide for Meeting Today's Underwriter Security Standards

Provided By Christensen Group Insurance

Use this guide to assess your current cybersecurity posture, identify gaps, and prepare for your next cyber insurance renewal or new policy submission.

1. Identity & Access Management (IAM)

Underwriters now treat MFA and privileged access controls as non-negotiables.

□ Multi-Factor Authentication (MFA) enabled for email, VPN/remote access, privileged accounts, and cloud applications (e.g., Microsoft 365, Google Workspace)
□ Unique user IDs and no shared credentials
□ Strong password policy (length, rotation, complexity)
□ Single Sign-On (SSO) implemented where possible
□ Privileged Access Management (PAM) in place for admin accounts
□ Least privilege enforced for all users

2. Endpoint Security & Device Protection

Most ransomware losses start at a compromised endpoint.

□ Endpoint Detection & Response (EDR) deployed across all servers & workstations
□ Full-disk encryption on all company laptops (e.g., BitLocker, FileVault)
□ Automated antivirus/anti-malware updates
□ Mobile device management (MDM) for phones/tablets accessing corporate data
□ Automated screen lockout and inactivity timeouts

3. Network Security

Underwriters expect layered network defenses—not just a firewall.

□ Next-gen firewall (NGFW) with IDS/IPS enabled
□ Network segmentation, separating critical assets from general traffic
□ Secure remote access (VPN with MFA or ZTNA)
□ Regular firewall rule reviews
□ Secure configuration standards for routers, switches, and wireless networks
□ Guest Wi-Fi isolated from internal business systems

Most organizations fail at least 25–40% of today's underwriting controls. That's where Christensen Group Insurance can help. Contact us today to request a personalized cyber insurance readiness assessment.

Christensen
Group
Insurance

4. Data Protection & Backups

Backup quality is now a top underwriting question.

□ Daily (or more frequent) backups of critical systems
□ Offsite or immutable/cloud-isolated backups
□ Backups encrypted in transit and at rest
□ Quarterly backup restoration testing
□ Defined data classification policy (PII, PHI, confidential, internal, public)
□ Formal data retention & destruction policies
□ (Optional) Secondary communication method for validating wire transfers/banking changes

5. Patch & Vulnerability Management

Outdated systems are one of the biggest red flags for insurers.

□ Formal patch management program
□ Critical patches applied within 14–30 days
□ Automated OS and application updates
□ Routine vulnerability scans (internal & external)
□ Inventory of all hardware/software assets (updated monthly)

6. Email Security & Anti-Phishing Controls

Email remains the #1 threat vector for business email compromise.

□ Advanced email filtering (phishing, spoofing, malware)
□ DMARC, DKIM, and SPF implemented and enforced
□ Anti-phishing warnings for external email senders
□ Secure email gateway or cloud email security add-on

7. Incident Response & Business Continuity

Underwriters want proof you are prepared—not just hoping for the best.

□ Documented Incident Response Plan (IRP)
□ IRP tabletop exercise conducted within the last 12 months
□ Logged cybersecurity incident history and remediation efforts
□ SIEM or centralized logging for security events
□ Documented Business Continuity & Disaster Recovery (BCP/DRP) plan
□ BCP/DRP testing conducted at least annually

Most organizations fail at least 25–40% of today's underwriting controls. That's where Christensen Group Insurance can help. Contact us today to request a personalized cyber insurance readiness assessment.

Christensen
Group
Insurance

8. Security Awareness & Training

Human behavior is still the most unpredictable security variable.

- □ Annual employee security awareness training
- □ Routine phishing simulation exercises
- □ Documented training participation records
- □ Role-based training for privileged users and executives

9. Vendor & Third-Party Risk Management

A weak vendor can jeopardize coverage—and your entire risk profile.

- □ Security assessments for critical vendors
- □ Vendor contracts requiring security standards & breach notification
- □ SOC 2 or ISO 27001 certification for key providers
- □ Documentation of data sharing and access rights
- □ Inventory of all vendors with network/data access

10. Policy, Governance, & Compliance Requirements

Insurers want administrative controls documented and regularly updated.

- □ Cybersecurity policies & procedures (acceptable use, data protection, remote work, etc.)
- □ Risk assessment reports (internal or third-party)
- □ Compliance documentation for applicable frameworks (NIST, CIS, SOC 2, ISO 27001, HIPAA, PCI DSS)
- □ Previous cyber insurance applications and claims history
- □ Records proving remediation of past weaknesses

Quick Self-Assessment Score

Count the number of items you checked:

40–47 = Strong underwriting posture

25–39 = Insurable, but improvements recommended

10–24 = High-risk; placement difficulty likely

0–9 = Requires foundational controls before obtaining coverage

Need Help Meeting These Requirements?

Our cyber insurance specialists provide coverage benchmarking, pre-application readiness reviews, underwriter-aligned cybersecurity roadmaps, access to vetted IT/security partners, and guidance on reducing premiums and improving insurability. Contact us today **(800-923-4088)** to request a personalized cyber insurance readiness assessment.

Christensen
Group
Insurance