APPALACHIA TECHNOLOGIES

CYBER INSURANCE READINESS

What Underwriters Actually Look For

Prepared by:

Appalachia Technologies

Your trusted technology advisor for AI strategy, cybersecurity, and GRC

appalachiatech.com

Cyber insurance applications are getting rejected at record rates - not because businesses are careless, but because underwriters have raised the bar on what 'protected' actually means. This checklist reflects **the eleven security controls underwriters may evaluate most often based on claims data and breach trends.**

Check each box if you can answer YES with confidence. Every 'No' is a gap that could cost you coverage - or raise your premium.

□ **Multi-Factor Authentication (MFA): Enforced on ALL administrative accounts and remote access**

- WHY IT MATTERS: Single-factor authentication is the #1 cause of credential-based breaches. Underwriters treat this as non-negotiable.

□ **Endpoint Detection & Response (EDR): Deployed on all workstations and servers**

- WHY IT MATTERS: Traditional antivirus isn't enough. EDR actively monitors for suspicious behavior and can contain threats before they spread.

□ **Email Security Filtering: Anti-phishing, anti-malware, link scanning in place**

- WHY IT MATTERS: Most ransomware starts with email. Underwriters want proof you're filtering at the gateway, not just relying on user judgment.

□ **Patching: Are all systems patched monthly?**

- WHY IT MATTERS: Unpatched vulnerabilities are a leading cause of breaches. Underwriters need assurance that you're staying ahead of known exploits.

□ **Vulnerability Scanning: Systems (internal and external) regularly scanned for vulnerabilities, misconfigurations, and missing patches**

- WHY IT MATTERS: Continuous scanning identifies exposure points before attackers do. It's a proactive measure, not a reactive fix.

□ **Penetration Testing: Are systems pentested at least once annually?**

- WHY IT MATTERS: Regular penetration testing identifies exploitable weaknesses that attackers could use to bypass defenses.

□ **Offsite, Encrypted Backups: Tested within the last 90 days**

- WHY IT MATTERS: 'We have backups' isn't enough. Can you prove they work? Offsite and immutable backups are now standard.

□ **Documented Incident Response (IR) Plan: Including designated IR contact or retainer**

- WHY IT MATTERS: When ransomware hits, who do you call? Underwriters want to see that you've answered that question before the incident happens.

□ **Privileged Access Review: Completed in the last 12 months**

- WHY IT MATTERS: Do you know who has admin rights? Many breaches succeed because overprivileged accounts go unmonitored.

□ **Security Awareness Training: Conducted at least annually (with phishing simulation)**

- WHY IT MATTERS: Your team is part of your security posture. Underwriters want to see that users are trained — and tested — on recognizing threats.

□ **No Prior Incidents (or Lessons Learned): No incidents in 3 years OR corrective actions documented for any prior breaches**

- WHY IT MATTERS: Past incidents aren't automatic disqualifiers - but failure to learn from them is. Underwriters look for evidence of corrective action.

APPALACHIA TECHNOLOGIES

YOUR SCORE

9-11 YES: Strong position. You're likely to pass underwriting with minimal friction.
6-8 YES: Moderate gaps. Expect questions and possibly higher premiums.
3-5 YES: At risk of rejection or significant premium increase. Address gaps before applying.
0-2 YES: High likelihood of rejection. Prioritize remediation before renewal.

WHAT TO DO NEXT

If You Have Gaps

Don't wait until renewal. Every 'No' on this checklist is a point of exposure - and underwriters know it. The good news: most of these controls can be implemented in 30-90 days with the right partner.

Start with MFA, EDR, and Patching. These are table stakes for modern cyber defenses.

Schedule Vulnerability Scans and Pen Tests. Regular testing takes you from reactive to proactive.

Test your backups.
Schedule a restore drill in the next 30 days. Document it; underwriters will ask for proof.

Build or update your IR plan. You don't need a 50-page manual. A one-page runbook with contact names and first-response steps is enough to start.

Run a security posture assessment. Bring in a third party to audit your environment and identify gaps.

Why This Matters Now

This checklist represents common controls that align with real breach trends and underwriter requirements. Not every underwriter evaluates these factors the same way, but organizations that address these areas will improve both their insurability and their true security posture.

Need Help Closing the Gaps?

Appalachia Technologies works with organizations in healthcare, financial services, defense contracting, and manufacturing to build the security controls underwriters expect - and to document them in ways that pass scrutiny.

Schedule a 30-minute Security Posture Review with our vCISO team. We'll walk through your current environment and identify your insurance readiness gaps.

appalachiatech.com | 888-277-8320 | info@appalachiatech.com

Managed. Protected. Compliance-Ready. Intelligent.