Are You Cyber Insurance Ready? A Readiness Checklist for Delaware Business Owners

Estimated read time: 7 minutes

If your Delaware business—whether you operate a professional law firm in Wilmington, a medical practice in Dover, or a growing financial consultancy in Newark—last applied for or renewed your cyber liability policy without a rigorous technical audit, you might be in for a rude awakening. Insurance underwriters have fundamentally changed the rules of the game. Legal and insurance analyses, including reporting from Law360, highlight a harsh reality: cyber insurance is no longer a safety net you can simply buy your way into. It is a highly scrutinized security compliance contract.

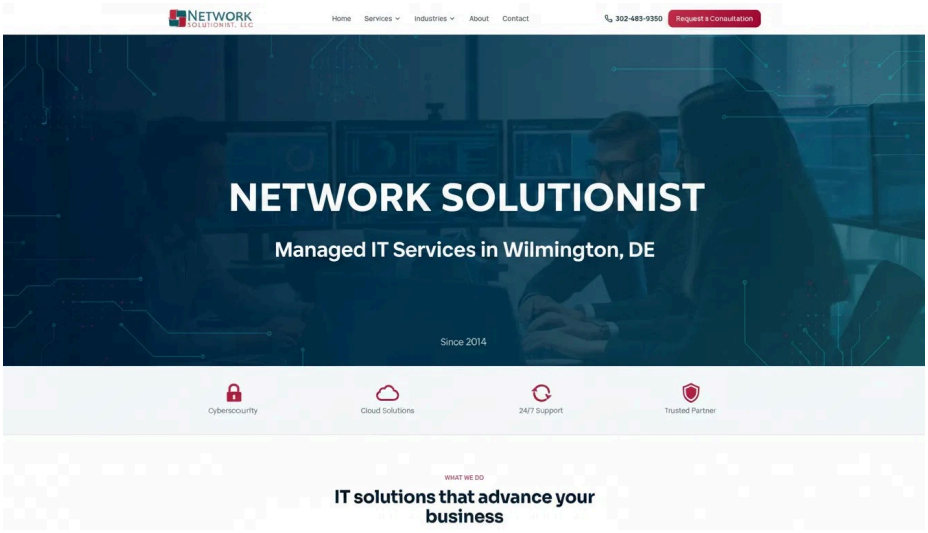
Carriers are rejecting claims, raising deductibles exponentially, and denying coverage outright for businesses that cannot empirically prove they have robust defensive controls in place. Answering "Yes" on a questionnaire without verifiable documentation is now treated as a material misrepresentation.

To help local organizations navigate this high-stakes landscape, we have broken down the core pillars of modern cyber insurance readiness. By aligning your on-premises infrastructure, cloud environments, and internal workflows with current underwriter expectations, you can protect your bottom line and ensure your policy actually pays out when disaster strikes.

---

1. Navigating Modern Cyber Insurance Questionnaires

Gone are the days when a simple four-question form would secure a million-dollar cyber policy. Today's applications resemble complex technical audits. Underwriters want granular proof of your security posture across workstations, servers, email platforms, and remote access gateways.



When filling out these questionnaires, precision is everything. If your IT provider or internal team checks "Yes" to advanced endpoint detection but your endpoints lack active behavioral monitoring, your policy could be voided after a breach.

Action Item: Conduct a comprehensive internal audit before your renewal window opens. Gather policy documents, network diagrams, and configuration reports. Do not guess—verify every single technical claim you submit to your broker.

---

2. Multi-Factor Authentication (MFA) Enforcement: The Non-Negotiable Standard

If there is one hill underwriters are willing to die on in 2026, it is Multi-Factor Authentication (MFA). Implementing basic MFA on your primary email account is no longer enough to check the box.

Carriers now demand comprehensive, enterprise-wide MFA coverage. This means enforcing secure authentication across:

- **All remote access points:** VPNs, Remote Desktop Protocol (RDP), Citrix, and administrative remote gateways.
- **Privileged accounts:** Domain administrators, local server admins, and firewall management consoles.
- **Cloud management consoles and productivity suites:** Microsoft 365, Google Workspace, AWS, and Azure.
- **Core business applications:** Document management systems, financial software, and client portals.

Furthermore, insurers are scrutinizing the *quality* of your MFA. Legacy SMS-based or voice-call verification methods are increasingly viewed as vulnerable due to SIM-swapping risks. Modern policies favor phishing-resistant MFA, such as hardware security keys (FIDO2) or authenticator app push notifications with number matching.

Action Item: Disable legacy authentication protocols (like POP and IMAP) that bypass MFA, and mandate conditional access policies so users cannot bypass security controls under any circumstances.

---

3. Backup Documentation & Immutable Storage: Defeating Ransomware

Ransomware syndicates know that modern businesses rely heavily on backups to recover from attacks. Consequently, attackers now make destroying or encrypting your backups their primary objective before triggering system-wide file locks.

To satisfy 2026 underwriter requirements, your backup strategy must go far beyond traditional nightly external hard drives or basic cloud syncs. Underwriters look for the strict application of the **3-2-1 backup rule**:

- **3** copies of your data across multiple formats.
- **2** different media types (e.g., local network storage and secure cloud repositories).
- **1** copy stored entirely **offsite and immutable**.

Immutable backups are tamper-proof files that cannot be modified, encrypted, or deleted by anyone—not even a compromised administrator account—for a predetermined retention period. If ransomware infiltrates your network, your immutable backups remain pristine and ready for restoration.

Action Item: Document your backup architecture, verify that your recovery point objectives (RPO) and recovery time objectives (RTO) align with your business continuity needs, and ensure backup administration credentials are completely segregated from standard domain credentials.

---

4. Incident Response Plans & Regular Restore Testing

Having a disaster recovery plan written in a Word document gathering digital dust is no longer sufficient. Underwriters require documented proof that your incident response plan (IRP) has been tested and that your backups actually work in practice.

Carriers frequently request logs and reports from recent restore tests. If your last backup restoration test was three years ago, your insurance claim could face severe delays or outright denial during a breach investigation.

Action Item: Schedule quarterly or at least semi-annual restore tests. Document the date, the specific systems restored, the time it took, and retain screenshots or logs confirming successful data recovery. Pair this with a clear, concise Incident Response Plan that outlines who to call—including your Managed Service Provider, legal counsel, and cyber insurance claims representative—within the first hour of a suspected intrusion.

Summary: The Short Version for Busy Business Owners

- **The questionnaire is a legal contract:** Never guess on a cyber insurance application. Inaccurate answers can lead to claim denials.

- **MFA must be universal:** Enforce phishing-resistant MFA across email, remote access, administrative accounts, and cloud platforms.
- **Backups must be immutable:** Ensure you have offline or immutable backup copies that ransomware cannot encrypt or delete.
- **Proof is mandatory:** Keep documented evidence of quarterly backup restore tests and updated incident response procedures.

Navigating the shifting demands of cyber insurance underwriters doesn't have to be an overwhelming burden for your team. Whether you need help hardening your infrastructure, upgrading to enterprise-grade MFA, or preparing your documentation packet, we are here to help.

To make this process seamless, download our **Free Cyber Insurance Readiness Checklist** today and evaluate your Delaware business against current carrier standards.

Download the Free Cyber Insurance Readiness Checklist Now

Ready to secure your network and breeze through your next policy renewal? Contact us today to schedule a comprehensive IT security assessment for your Wilmington, Newark, Dover, Middletown, or Rehoboth office. Let us handle the technical complexities so you can focus on growing your business.

Network Solutionist, LLC | info@nsolutionist.com | 302-485-9850