THREATNEXIS | SMALL BUSINESS CYBERSECURITY

Cyber Insurance Readiness Checklist

Know What Insurers Require Before You Apply — and Pass with Confidence

$1.8M
Average cyber claim paid in 2024 for SMBs with coverage

62%
of SMB cyber claims are denied due to misrepresented controls

3x
higher premiums for businesses that cannot demonstrate basic security controls

FREE EDITION | threatnexis.com | 2025 Edition | For businesses with 1–250 employees

What's Inside This Checklist

- Why cyber insurance claims get denied
- What underwriters actually look for
- 8 critical security control categories
- 60+ specific checklist items with insurer status
- How to read and understand your policy
- Coverage types and what they actually cover
- Common policy exclusions to watch for
- Quick wins to improve your readiness today

1. Overview

Cyber insurance is no longer optional for small businesses. It is the financial safety net that keeps a ransomware attack or data breach from becoming a business-ending catastrophe. But cyber insurance only works if your claim gets paid — and an alarming number of claims are denied because businesses misrepresented their security controls at the time of application, or failed to maintain those controls after the policy was issued.

This checklist gives you a clear picture of what underwriters actually require, what they look for during audits, and where the most common gaps are for small businesses. Work through each section before applying for coverage, at renewal, and any time you make significant changes to your technology environment.

2. Why This Matters

REAL-WORLD CLAIM DENIAL SCENARIO

A manufacturing firm in Texas paid $18,000 per year for cyber insurance. When ransomware hit and the recovery cost reached $340,000, their claim was denied. The reason: the application had indicated MFA was enabled on all admin accounts. It wasn't. The policy was voided for material misrepresentation. They received nothing.

The Three Ways Cyber Claims Fail

1. Material Misrepresentation	2. Policy Exclusions	3. Control Drift
You stated on the application that controls were in place that weren't. Insurers can void the policy entirely.	The incident type (e.g., war, nation-state, unencrypted devices) is explicitly excluded from your policy.	Controls were in place at application but were later disabled, not maintained, or not extended to new systems.

3. What Underwriters Actually Look For

Cyber underwriters are becoming increasingly technical. Many now use scanning tools to assess your external attack surface before quoting. Others send detailed questionnaires covering specific security controls. Here is what they prioritize, in order of importance:

Rank	Security Control	Why Underwriters Care
#1	**Multi-Factor Authentication (MFA)**	The single most important control. MFA on email and remote access prevents the majority of credential-based attacks. Absence is a hard disqualifier at most carriers.
#2	**Backups (Immutable, Tested, Offline)**	Without tested backups, ransomware becomes a business-ending event. Insurers know that organizations with tested backups recover; those without often don't.
#3	**Endpoint Detection & Response (EDR)**	EDR provides the visibility and response capability to contain incidents before they become catastrophic claims. Basic AV is no longer sufficient.
#4	**Email Security (Filtering + DMARC)**	91% of attacks start with phishing. Insurers look for filtering, anti-phishing controls, and properly configured DMARC to prevent spoofing of your domain.
#5	**Privileged Access Controls**	Admin account compromise is the pivot point in most ransomware attacks. Insurers want to see MFA on admin accounts, least-privilege access, and no shared admin credentials.
#6	**Patch Management**	Unpatched systems are the easiest target. Insurers expect a documented patch process with critical patches applied within 30 days.
#7	**Incident Response Plan**	A documented, tested IR plan demonstrates preparedness and reduces claim severity. Insurers increasingly require evidence of this.
#8	**Security Awareness Training**	Human error causes 82% of breaches. Insurers want evidence of regular phishing-resistant training for all staff.

4. The Cyber Insurance Readiness Checklist

Work through each section of this checklist before applying for or renewing your cyber insurance policy. Update your "Your Status" column honestly — misrepresenting controls on an application can void your entire policy.

Required — Hard disqualifier if absent	Increasingly Required — Growing expectation	Recommended — Improves terms / reduces premium

01 Identity & Access Management

MFA, privileged access, and credential security

☐	Requirement	Insurer Status	Your Status
☐	Multi-Factor Authentication (MFA) enabled on all email accounts	**Required**	Yes / No / Partial

☐	MFA enabled on all remote access (VPN, RDP, remote desktop tools)	**Required**	Yes / No / N/A
☐	MFA enabled on all administrator and privileged accounts	**Required**	Yes / No / Partial
☐	No shared administrator credentials across multiple staff	**Required**	Yes / No
☐	Password manager deployed for all employees	**Increasingly Required**	Yes / No
☐	Password policy enforces minimum length of 12+ characters	**Increasingly Required**	Yes / No
☐	Least-privilege access: employees only access systems they need	**Increasingly Required**	Yes / No / Partial
☐	Inactive user accounts disabled or removed within 24 hours of departure	**Recommended**	Yes / No
☐	Administrator accounts are separate from standard user accounts	**Recommended**	Yes / No

02 Email Security

Anti-phishing, filtering, and domain authentication

☐	Requirement	Insurer Status	Your Status
☐	Email filtering solution deployed (not just spam filter)	**Required**	Yes / No
☐	Anti-phishing policies configured for all users	**Required**	Yes / No / Partial
☐	SPF DNS record published for your email domain	**Required**	Yes / No
☐	DKIM signing enabled and DNS record published	**Required**	Yes / No
☐	DMARC DNS record published with at least p=quarantine policy	**Increasingly Required**	Yes / No
☐	Safe Links / URL rewriting active on all email accounts	**Increasingly Required**	Yes / No
☐	Safe Attachments / sandbox detonation enabled	**Increasingly Required**	Yes / No
☐	External email warning banners configured	**Recommended**	Yes / No
☐	Automatic email forwarding to external domains blocked	**Recommended**	Yes / No

03 Endpoint Security

EDR, patching, and device controls

☐	Requirement	Insurer Status	Your Status
☐	Endpoint Detection & Response (EDR) deployed on all workstations	**Required**	Yes / No / Partial
☐	EDR deployed on all servers (on-premise and cloud)	**Increasingly**	Yes / No /

		Required	Partial
☐	Antivirus / anti-malware active on all devices	**Required**	Yes / No
☐	Operating system patches applied within 30 days of release	**Required**	Yes / No / Partial
☐	Critical/security patches applied within 14 days of release	**Increasingly Required**	Yes / No / Partial
☐	Third-party application patches applied within 30 days	**Increasingly Required**	Yes / No / Partial
☐	No end-of-life operating systems in production use	**Required**	Yes / No
☐	Removable media / USB storage restricted or blocked	**Recommended**	Yes / No
☐	Full-disk encryption enabled on all laptops and mobile devices	**Increasingly Required**	Yes / No / Partial

04 Backup & Recovery

Ransomware-proof backup and tested recovery

☐	Requirement	Insurer Status	Your Status
☐	All critical data backed up daily	**Required**	Yes / No / Partial
☐	Backups stored offsite or in a separate cloud environment	**Required**	Yes / No
☐	Backups are immutable (cannot be deleted or encrypted by ransomware)	**Required**	Yes / No
☐	Backups are isolated from the primary network (air-gapped or separate tenant)	**Required**	Yes / No / Partial
☐	Backup restoration tested within the past 90 days	**Increasingly Required**	Yes / No
☐	Recovery Time Objective (RTO) and Recovery Point Objective (RPO) defined	**Increasingly Required**	Yes / No
☐	Microsoft 365 / Google Workspace data backed up separately (not just synced)	**Increasingly Required**	Yes / No
☐	Backup access protected by MFA and separate credentials	**Recommended**	Yes / No

05 Network & Remote Access Security

VPN, firewall, and network segmentation

☐	Requirement	Insurer Status	Your Status
☐	Business-grade firewall deployed and actively managed	**Required**	Yes / No
☐	VPN or Zero Trust solution required for all remote access	**Required**	Yes / No
☐	RDP (Remote Desktop Protocol) not exposed directly to the internet	**Required**	Yes / No

☐			
☐	Network segmentation: guest/IoT networks separated from business network	Increasingly Required	Yes / No / Partial
☐	DNS filtering active to block malicious domains	Increasingly Required	Yes / No
☐	Unnecessary ports and services disabled on internet-facing systems	Increasingly Required	Yes / No / Partial
☐	Wireless networks encrypted with WPA3 or WPA2-Enterprise	Recommended	Yes / No
☐	Security logging / SIEM enabled for network events	Recommended	Yes / No

06 Incident Response & Governance

IR plan, policies, and documentation

☐	Requirement	Insurer Status	Your Status
☐	Written Incident Response (IR) plan exists and is current	Increasingly Required	Yes / No
☐	IR plan has been tested via tabletop exercise within the past year	Increasingly Required	Yes / No
☐	Incident response roles assigned to named individuals	Increasingly Required	Yes / No
☐	Acceptable Use Policy (AUP) in place and signed by all employees	Recommended	Yes / No
☐	Password policy documented and enforced	Recommended	Yes / No
☐	Remote Work / BYOD policy documented and communicated	Recommended	Yes / No
☐	Vendor / Third-Party security review process in place	Increasingly Required	Yes / No / Partial
☐	Software/hardware asset inventory maintained and current	Increasingly Required	Yes / No / Partial
☐	Cyber insurance policy reviewed and understood by leadership	Recommended	Yes / No

07 Security Awareness & Training

Phishing resistance and security culture

☐	Requirement	Insurer Status	Your Status
☐	Annual security awareness training delivered to all employees	Required	Yes / No
☐	Phishing simulation tests conducted at least annually	Increasingly Required	Yes / No
☐	Business Email Compromise (BEC) wire transfer verification process in place	Required	Yes / No
☐	New employee security onboarding training in place	Increasingly Required	Yes / No

☐	Employees trained to report suspicious emails and activity	Recommended	Yes / No
☐	Security awareness content updated annually for current threats	Recommended	Yes / No

08 Vendor & Third-Party Risk

Supply chain and partner security

☐	Requirement	Insurer Status	Your Status
☐	Inventory of all third-party vendors with system access maintained	Increasingly Required	Yes / No / Partial
☐	Vendor security questionnaires or reviews conducted annually	Increasingly Required	Yes / No / Partial
☐	Business Associate Agreements (BAA) in place for healthcare vendors	Required (Healthcare)	Yes / No / N/A
☐	Vendor access limited to least-privilege and time-bounded where possible	Recommended	Yes / No / Partial
☐	Contracts with key vendors include security and breach notification clauses	Recommended	Yes / No / Partial
☐	Software supply chain risk considered when adopting new tools	Recommended	Yes / No / Partial

5. Understanding Cyber Insurance Coverage

Not all cyber policies are the same. Understanding the coverage types ensures you have the right protection — and aren't surprised when a claim is filed.

Coverage Type	What It Covers	Watch For
First-Party Coverage	Your own costs: IR response, forensics, notification, credit monitoring, business interruption, ransom payments	Sub-limits on ransomware and BI coverage; waiting periods
Third-Party Liability	Claims from clients/partners for your data breach or failure that impacted them	Coverage limits may not match your client contract requirements
Business Email Compromise	Fraudulent funds transfer resulting from social engineering	Often a separate sub-limit; many businesses dramatically underestimate exposure
Ransomware / Extortion	Ransom payments and IR costs related to ransomware events	Nation-state exclusions; may require proof of backups; sub-limits

Business Interruption	Lost revenue and extra expenses when systems are down	Waiting periods (12–48+ hours); may require specific triggers
Regulatory Defense	Legal costs and fines related to HIPAA, PCI, state breach notification	Some policies exclude known regulatory violations at time of purchase
Media Liability	Claims related to online content, defamation, or copyright infringement	Often overlooked; relevant for businesses with active online presence

POLICY READING TIP

Always read your policy's definitions section carefully. The definition of "computer fraud," "funds transfer fraud," and "electronic theft" varies significantly between carriers — and the difference can be worth hundreds of thousands of dollars at claim time.

6. Common Policy Exclusions to Watch For

Exclusions are the clauses in your policy that explicitly define what is NOT covered. Review these with your broker before purchasing and ensure you understand each one.

War & Nation-State Exclusion

Most policies exclude attacks attributed to nation-state actors or acts of cyberwarfare. This exclusion has been contested in court and is being actively litigated. Ask your broker specifically how this is defined and what evidence would be required to invoke it.

Prior Acts / Known Claims Exclusion

Incidents that occurred or were discovered before the policy inception date are not covered. If you suspect a breach at the time of application, disclose it to your broker — concealment is grounds for denial.

Unencrypted Data Exclusion

Some policies exclude claims involving unencrypted data, particularly on lost or stolen devices. Enable full-disk encryption on all laptops and mobile devices — this is now a basic insurer expectation.

Failure to Maintain Controls

If you stated on your application that specific controls were in place and they are found to be absent at the time of a claim, the insurer may deny the claim or void the policy entirely. Audit your controls at every renewal.

Social Engineering Sub-Limits

Many policies have significantly lower sub-limits for social engineering and BEC fraud than for other incident types. Businesses often discover this limitation after suffering a $200,000 wire fraud and finding their BEC coverage is capped at $25,000.

⚠ **Bodily Injury / Property Damage**

Standard cyber policies do not cover physical harm caused by a cyberattack (e.g., a compromised medical device). Industries with operational technology or medical devices need specialized coverage.

7. Quick Wins: Improve Readiness Today

These five actions have the highest impact on your insurability, your premium cost, and the likelihood your claim gets paid. None require significant budget.

#	Action	Impact	Cost
01	Enable MFA on all Microsoft 365 accounts via Security Defaults. This is the single most scrutinized control by every cyber underwriter.	Critical	Free
02	Verify your backup is actually restorable. Restore a test file from your most recent backup today. Document the date and result.	Critical	Free
03	Run your domain through mxtoolbox.com — check SPF, DKIM, and DMARC. Fix any failures before your next renewal.	High	Free
04	Document your incident response plan, even as a single page. Name the Incident Commander, IT contact, insurance carrier, and attorney.	High	Free
05	Pull out your cyber policy and find the BEC/social engineering sub-limit. If it is under $100,000, call your broker before next renewal.	High	Free

8. Resources & Next Steps

Helpful External Resources

- Coalition Cyber Insurance (direct carrier with free cyber risk assessment): coalitioninc.com
- Corvus Insurance (SMB-focused, security score-based pricing): corvusinsurance.com
- MxToolbox Email Authentication Check: mxtoolbox.com

- CISA Cyber Insurance Resources: cisa.gov/cyber-insurance
- FTC Cybersecurity for Small Business: ftc.gov/smallbusiness
- IC3 Cyber Crime Reporting (FBI): ic3.gov

THREATNEXIS INSIGHT

Cyber insurance is not a substitute for good security — it is a backstop for the residual risk you cannot eliminate. The best cyber insurance strategy is: implement strong controls, document everything, and buy coverage that matches your actual risk profile.

SEO & Content Strategy Reference

Primary Keyword:

- cyber insurance readiness checklist small business

Secondary Keywords:

- what do cyber insurers require
- cyber insurance application requirements
- how to get cyber insurance small business
- cyber insurance claim denied MFA
- cyber insurance controls checklist 2025

SEO Title:

- Cyber Insurance Readiness Checklist for Small Business: 60+ Requirements [2025]

Meta Description:

- Know exactly what cyber insurers require before you apply. Free checklist covering MFA, backups, EDR, email security, and 60+ specific controls with insurer requirement status.

SEO Slug:

- /cyber-insurance-readiness-checklist-small-business

People Also Ask:

- What security controls do cyber insurers require?
- Why was my cyber insurance claim denied?
- Does my small business need cyber insurance?
- What is the average cost of cyber insurance for small businesses?
- What is material misrepresentation in a cyber insurance policy?

Monetization Opportunities:

- Premium Cyber Insurance Readiness Toolkit (premium version of this guide)
- Cyber Insurance Readiness Assessment Consulting Service

- Security Gap Remediation Package (fix gaps before renewal)
- Virtual CISO Retainer — ongoing compliance and insurer readiness
- Microsoft 365 Security Configuration Service

Want the Complete Small Business Security Toolkit?

The Threatnexis Premium Toolkit includes industry-specific readiness assessments, gap remediation plans, underwriter scorecards, and more:

- ✓ Full Underwriter Scorecard & Gap Analysis
- ✓ Industry-Specific Readiness Packages
- ✓ 90-Day Gap Remediation Roadmap
- ✓ Policy Comparison Worksheet
- ✓ Carrier Application Answer Guide
- ✓ Broker Interview Preparation Guide
- ✓ Evidence Documentation Templates
- ✓ Board-Ready Insurance Summary Report

➤ **[Unlock the Premium Cyber Insurance Readiness Toolkit at threatnexis.com]**

Need a Cyber Insurance Readiness Review?

Threatnexis Consulting reviews your security controls, identifies gaps, and helps you apply with confidence.

➤ **[Book a Free Consultation]**

Join the Threatnexis Insider Community

Monthly checklists, templates, security tips, and new downloads — always free.

➤ **[Subscribe Free]**