FREE RESOURCE · 2026 EDITION

THE ADJUSTER'S CHECKLIST

# 12 Things I Looked for Before Approving a Cyber Insurance Claim

## What every SMB owner needs to know before a breach, from someone who sat on the other side of the claims desk.

After years evaluating cyber insurance claims at a large carrier, I know exactly which gaps adjusters flag, and which controls turn a disputed claim into a paid one. This checklist is not a generic security framework. It is built around the specific questions an adjuster asks when your claim lands on their desk.

| 40%+ | 82% | 7 |
|---|---|---|
| of cyber claims denied or reduced at payout | of denials tied to missing or weak MFA | checklist sections matched to adjuster criteria |

*Sources: Delinea 2024 Cyber Insurance Report · SentinelOne Cybersecurity Statistics 2026 · Protectyr Cyber Insurance Readiness Research 2025*

### HOW TO USE THIS CHECKLIST

Go through each section with your IT lead, office manager, or GRC consultant. Check the box only if the control is fully in place, not partially, not "in progress." Any unchecked item is a potential gap your insurer may flag during a claim investigation.

SECTION 01

## Access Controls & Authentication

- [ ] **Multi-Factor Authentication (MFA) on email**
  All staff, not just admins. Email is the #1 breach entry point.
- [ ] **MFA on all cloud platforms and remote access**
  Microsoft 365, Google Workspace, VPNs, RDP, and cloud storage.
- [ ] **MFA on admin and privileged accounts**
  Separate admin accounts with MFA; no shared admin credentials.
- [ ] **Password policy enforced**
  Minimum 12 characters; no reuse; documented and acknowledged by staff.
- [ ] **Inactive and former employee accounts disabled promptly**
  Terminated employee access removed within 24 hours of departure.

SECTION 02

## Incident Response Preparedness

- [ ] **Written Incident Response Plan (IRP) in place**
  Dated, version-controlled, and stored where staff can access it during an incident.
- [ ] **IRP includes insurer notification requirement**
  Carriers must be notified within the policy window, often 24-72 hours.
- [ ] **Named Incident Response Lead assigned**
  One person owns coordination. Not a committee, a named individual.
- [ ] **Tabletop exercise completed in the last 12 months**
  Walk through a simulated breach. Document who attended and when.
- [ ] **Forensic vendor pre-selected (carrier-approved preferred)**
  Engaging an unapproved vendor can create coverage complications.

SECTION 03

## Backup & Recovery

- [ ] **Backups running on all critical systems**
  Frequency matches your recovery time objective (RTO).

- [ ] **Backups stored offsite or in isolated cloud environment**
  Backups on the same network as production data can be encrypted in a ransomware event.

- [ ] **Backup restoration tested within the last 6 months**
  Untested backups are not evidence of recovery capability. Document the test date and result.

- [ ] **Recovery time documented and communicated**
  Know how long restoration actually takes, not an estimate.

SECTION 04

## Endpoint & Network Security

- [ ] **Endpoint Detection & Response (EDR) on all devices**
  Standard antivirus is no longer sufficient for most carriers. EDR is now a baseline requirement.

- [ ] **Patch management policy in place**
  Critical patches applied within 30 days. Document patching cadence.

- [ ] **Email filtering and anti-phishing controls active**
  Phishing is the most common incident trigger. Filtering alone is not enough without training.

- [ ] **Network segmentation in place for sensitive data**
  Critical systems should not share a flat network with general staff workstations.

SECTION 05

## Documentation & Policy

- [ ] **Acceptable Use Policy (AUP) in place and signed**
  Employees and contractors must acknowledge it in writing. Undated acknowledgments carry limited weight.

- [ ] **Data Handling Policy defines what data you collect and how**
  Carriers want to see that you know what sensitive data you hold and where it lives.

- [ ] **Vendor / Third-Party Risk policy or process exists**
  Third-party access is a top breach vector. Document how vendors are vetted and what access they have.

- [ ] **AI Use Policy in place (if staff use AI tools)**
  Increasingly reviewed during underwriting. Covers data input restrictions and approved tools.

- [ ] **All policies version-controlled with dates**
  An undated policy is difficult to use as evidence. Version number + effective date on every document.

SECTION 06

## Security Awareness Training

- [ ] **Annual security awareness training completed by all staff**
  Training records must exist: names, dates, topics covered.

- [ ] **Phishing simulation conducted in the last 12 months**
  Simulation results are increasingly requested during underwriting.

- [ ] **Training covers social engineering and business email compromise**
  BEC and wire fraud are among the most common covered losses.

- [ ] **New employee training completed within 30 days of hire**
  A lapse in onboarding training is a documented gap.

SECTION 07

## Insurance Application Accuracy

- [ ] **Application answers reviewed against actual controls in place**
  Misrepresentation, even unintentional, is the most common basis for claim denial.

- [ ] **Policy application retained on file**
  You need your original answers if a claim is disputed.

- [ ] **Coverage limits and exclusions reviewed annually**
  Social engineering, war, and nation-state exclusions are common blind spots.

- [ ] **Insurer notification obligations known and documented**
  Who calls the carrier? When? What information do they need? This should be in your IRP.

- [ ] **Prior claims or incidents disclosed accurately**
  Non-disclosure of known incidents prior to policy start is grounds for rescission.

FROM THE ADJUSTER'S DESK

# Five Things That Get Claims Denied (That Nobody Tells You)

## 1. The application said yes. The controls said no.

If your cyber insurance application checked 'MFA enforced' but MFA wasn't active on the compromised account at the time of the incident, that discrepancy is documented grounds for denial. Adjusters compare your application answers to forensic findings. Every mismatch is a question that has to be answered.

## 2. You called IT before you called your insurer.

Most policies require you to notify your carrier within 24-72 hours of discovering an incident. Bringing in outside IT vendors, issuing a public statement, or cleaning up systems before the carrier knows about the incident can create serious coverage complications, and in some cases, forfeit your right to use carrier-approved vendors, which affects reimbursement.

## 3. The backup existed. The restoration didn't.

Adjusters don't ask 'do you have backups?' They ask for evidence that backups were tested and that recovery was verified. A backup service running in the background with no documented restoration test is not recoverable proof of business continuity.

## 4. The policy was written. Nobody had read it.

Acceptable use policies, incident response plans, and data handling policies only protect you if they were in place, acknowledged by staff, and dated before the incident occurred. A policy created after a breach, or one without employee acknowledgment records, carries almost no evidentiary weight.

## 5. The incident happened. The notification didn't.

Late reporting is one of the most common, and most avoidable, claim complications. Know your policy's notification window before something goes wrong. It should be written into your incident response plan so the person handling the incident doesn't have to find the policy document in the middle of a crisis.

SCORING GUIDE

| Boxes Checked | What It Means | Recommended Next Step |
|---|---|---|
| 30-32 ✓ | Strong readiness posture | Annual review and document retention. Consider a retainer for ongoing support. |
| 22-29 ■ | Moderate gaps present | A Readiness Audit will identify and prioritize the specific gaps. |
| Under 22 ✗ | Material gaps present | High claim denial risk. A Readiness Package closes gaps before your next application or renewal. |

## Ready to Close Your Gaps?

This checklist shows you where you stand. A Readiness Engagement shows you exactly what to fix, and produces the documentation your insurer needs to see.

**Readiness Audit · $500**

Gap analysis against underwriter requirements. Written findings, risk ratings, and a prioritized action list. 5-7 business days.

**Readiness Package · $1,500**

Full risk assessment plus 3 core policy documents (AUP, IRP, Data Handling) and an executive summary for your insurer. 2-3 weeks.

**Monthly Retainer · $800/mo**

Ongoing GRC support, policy updates, vendor risk reviews, and annual renewal prep. 3-month minimum.

**Book a Free 30-Minute Discovery Call**

**support@technicalterminator.com · technicalterminator.com**

*Technical Terminator LLC is a GRC and cyber insurance readiness consultancy serving small and mid-size businesses in Dallas-Fort Worth, Texas. This checklist is provided for informational purposes only and does not constitute legal, insurance, or compliance advice. Controls and underwriter requirements vary by carrier and policy.*