PHANTOM
Technology Solutions

PHANTOM TECHNOLOGY SOLUTIONS · CHECKLIST

# Is your business actually insurable?

A practical self-audit covering the 24 controls cyber insurance carriers are asking about in 2026 — with the ones most likely to deny a claim if you get them wrong.

CYBER INSURANCE

SECURITY CONTROLS

SELF-AUDIT

# Before you renew, read this.

Cyber insurance underwriters have tightened requirements every year since 2021. Most denied claims aren't denied because of what happened — they're denied because the business attested to controls on their application that weren't actually in place at the time of the incident. This checklist walks you through the 24 controls carriers ask about most often, grouped by the four questions they're really trying to answer.

> How to use this: Check each box your business can honestly, verifiably confirm today. Any unchecked item is a gap — either fix it before your next renewal, or disclose it accurately on your application.

## 1. Can you prove who's in your environment?

- ☐ Multi-factor authentication (MFA) is enforced on all email accounts
- ☐ MFA is enforced on all remote access (VPN, RDP, or equivalent)
- ☐ MFA is enforced on all privileged / administrator accounts
- ☐ MFA is enforced on all cloud apps containing sensitive data
- ☐ A documented process exists to offboard users within 24 hours of departure
- ☐ Shared or generic admin accounts have been eliminated or vaulted

## 2. Can you detect and stop an intrusion?

- ☐ Endpoint Detection & Response (EDR) is deployed on every endpoint, including servers
- ☐ EDR is monitored 24/7 by a Security Operations Center (SOC) or MDR provider
- ☐ Email security filters block phishing, impersonation, and malicious attachments
- ☐ DNS filtering or web filtering is enforced on endpoints
- ☐ Local administrator rights have been removed from standard user accounts
- ☐ Critical security patches are applied within 14 days of release

## 3. Can you recover without paying the ransom?

- ☐ Backups are automated, daily, and include all critical systems
- ☐ At least one backup copy is immutable or air-gapped (not writable from production)
- ☐ Backups are tested by full restore at least quarterly
- ☐ A written incident response plan exists and has been reviewed in the last 12 months
- ☐ The IR plan has been tabletop-tested with leadership in the last 12 months
- ☐ You have contact information for a breach coach, forensics firm, and carrier hotline

## 4. Can you prove you're doing the work?

- ☐ A written information security policy exists and is reviewed annually
- ☐ Security awareness training is delivered to all employees annually
- ☐ Simulated phishing tests are run at least quarterly
- ☐ A written vendor / supply chain risk review process is in place
- ☐ Security roles and responsibilities are documented and assigned
- ☐ An IT asset inventory is maintained and updated regularly

## How did you score?

| | |
|---|---|
| 22–24 checked | Strong. You're in line with what most carriers expect in 2026. Use your documentation as leverage at renewal. |
| 17–21 checked | Coverage-eligible but exposed. Close the gaps before renewal — especially MFA, EDR/MDR, and immutable backups. |
| Under 17 checked | High risk. Many carriers will non-renew or exclude ransomware. Prioritize a formal assessment before your next application. |

## Next step

If you checked fewer than 22 boxes — or you're not sure — request a free Cyber Risk Report at phantomts.com. We'll map your environment against the same 24 controls above and show you exactly where you stand, in under 24 hours, at no cost.