

Cyber Insurance Assessment Checklist



A practical guide for small business owners to discover what their cyber insurance really covers.

computercare
Aligning technology, delivering success.

How to Use This Checklist

Step 1: Get your cyber insurance policy (the actual policy document, not the summary)

Step 2: Go through each section below and check YES or NO

Step 3: Count your NO answers - each one is a potential gap

Step 4: Use the action steps at the end to fix what you find

Don't panic if you find gaps - most businesses have them. The important thing is knowing about them before you need to make a claim.

Section 1: Policy Basics (Do You Know What You Bought?)

- I have read my entire cyber insurance policy

The full policy document with all the fine print

- I have budgeted for my excess and know when it applies

Can you afford to pay this amount out of pocket before insurance kicks in?

- My policy has coverage limits for different types of incidents

Different types of cyber incidents often have different maximum payouts

- I have a current copy of my policy easily accessible, printed out

You'll need this immediately if something happens - don't hunt for it during a crisis

- I know when my policy expires and have renewal reminders set

Gaps in coverage can void claims even for incidents that happened while covered

Red Flag: If you checked NO to any of these, you're flying blind with your coverage.

Section 2: The Sneaky Exclusions (What WON'T Be Covered)

- My policy covers incidents involving artificial intelligence or automated attacks**

Many policies exclude AI-driven attacks - this is becoming more common

- My policy covers attacks that come through my suppliers or vendors**

Third-party incidents are often excluded but can still devastate your business

- My policy covers "acts of war" or nation-state attacks**

If hackers are linked to foreign governments, many policies walk away

- My policy covers social engineering attacks (like fake wire transfers)**

Someone tricks your employee into sending money - is this covered?

- My policy covers attacks on my cloud services (Office 365, Google Workspace, etc.)**

Whose responsibility is cloud security - yours or your provider's?

- My policy covers regulatory fines and penalties**

Getting hacked might trigger government fines - will insurance pay them?

- My policy covers business interruption from cyber incidents**

If you can't operate for weeks, will insurance cover your lost income?

Red Flag: Each NO here is a potential denial waiting to happen.

Section 3: Security Requirements (The Fine Print That Kills Claims)

- I know exactly what security measures my policy requires me to have

Most policies have a list of "must-haves" buried in the fine print

- All my business accounts have multi-factor authentication (MFA) in use

This is becoming a universal requirement - no MFA often means no payout

- I have endpoint protection (antivirus & EDR) on all business devices

Basic requirement that many businesses miss on some devices

- All my business software is kept up to date with the latest security patches

Using outdated software can void your coverage

- I have regular backups that are fully tested and stored securely

"Regular" and "tested" are key - old or broken backups don't count

Tested means that you can fully recover to a clean / new system, not just restore some files.

- I have documented cybersecurity policies and conduct regular employee training

Many policies require proof that you trained employees on security

- I conduct regular security assessments or audits

Some policies require annual security reviews

Red Flag: Missing any required security measures can void your ENTIRE policy.

Section 4: Coverage Gaps (What Might Fall Through the Cracks)

- My policy covers ransom payments (if I choose to pay)**

Some policies exclude ransom payments entirely

- My policy covers the cost of negotiating with hackers**

Specialized negotiators are expensive but often necessary

- My policy covers forensic investigation costs**

Finding out how you got hacked and fixing it costs thousands

- My policy covers legal fees for customer lawsuits**

Customers might sue you if their data was compromised

- My policy covers credit monitoring for affected customers**

You might be legally required to provide this

- My policy covers public relations and crisis management**

Protecting your reputation after a breach costs money

- My policy covers the cost of complying with data breach notification laws**

Notifying customers and regulators about breaches has specific requirements

Red Flag: These "extras" can cost more than the initial hack.

Section 5: Real-World Scenarios (Will You Actually Get Paid?)

Scenario A: Employee Falls for Phishing Email

Someone clicks a bad link and hackers get into your system

- This would be covered under my policy I'm not sure if this would be covered

Scenario B: Ransomware Attack via Remote Work Setup

Hackers get in through an employee working from home

- This would be covered under my policy I'm not sure if this would be covered

Scenario C: Customer Data Stolen from Cloud Service

Your customer database in the cloud gets breached

- This would be covered under my policy I'm not sure if this would be covered

Scenario D: Wire Transfer Fraud

Someone tricks your bookkeeper into wiring money to criminals

- This would be covered under my policy I'm not sure if this would be covered

Scenario E: System Down for Two Weeks

You can't operate your business due to a cyber incident

- Lost income would be covered under my policy I'm not sure if lost income would be covered

Red Flag: If you answered "I'm not sure" to any scenario, you need clarification BEFORE something happens.

Section 6: Claims Process (Do You Know How to Actually Get Help?)

- I know exactly who to call if a cyber incident happens

Do you have a 24/7 number? Is it programmed into key people's phones?

- I know what documentation I need to keep for a claim

Screenshots, logs, communications - what evidence do you need?

- I understand the timeline for reporting incidents

Most policies require notification within 24-72 hours

- I know what I'm allowed to do (and not do) before calling insurance

Some actions can void your claim if done before notifying the insurer

- I have contact information for recommended incident response providers

Many policies require you to use approved vendors

Red Flag: Not knowing the claims process can turn a covered incident into a denied claim.

Your Gap Assessment Score

Count your total NO answers and "I'm not sure" responses:

- **0-5 Gaps:** You're in better shape than most, but still review those gaps
- **6-15 Gaps:** You have significant coverage risks that need attention
- **16-25 Gaps:** Your coverage has serious holes that could be catastrophic
- **26+ Gaps:** You're essentially unprotected despite paying premiums

Question	Answer
1	
2	
3	
4	
5	
6	
7	
8	

Action Steps Based on Your Results

If You Found 0-5 Gaps:

- ✓ Schedule a policy review with your broker to confirm your understanding
- ✓ Document your security measures to prove compliance if needed
- ✓ Create an incident response plan with clear steps and contacts

If You Found 6-15 Gaps:

- ◆ Schedule an urgent meeting with your insurance broker to discuss gaps
- ◆ Consider additional coverage for major exclusions you discovered
- ◆ Implement missing security requirements immediately
- ◆ Get quotes from other insurers to compare coverage options

If You Found 16+ Gaps:

- 🚨 Treat this as an emergency - you're paying for coverage you don't have
- 🚨 Don't wait - start shopping for new coverage immediately
- 🚨 Implement basic security measures this week to reduce immediate risk
- 🚨 Consider cyber security consulting to properly assess and fix your risks

Questions to Ask Your Insurance Broker

Use these exact questions - don't let them give you vague answers

1. "Can you show me exactly where in my policy it covers [specific scenario]?"
2. "What security measures am I required to maintain, and where is this documented?"
3. "If I have a claim, what documentation will I need to provide?"
4. "What's the maximum my policy will pay for [specific type of incident]?"
5. "Are there any exclusions that would apply to my type of business?"
6. "What happens if I don't meet the security requirements?"
7. "Can you give me examples of similar claims that were denied and why?"

Free Resources

If you found gaps in your coverage:

- Follow us on LinkedIn
- Keep an eye out for our next free webinar
- Sign up to our monthly newsletter where we discuss cyber security and other technology topics.
- Email us for our "Cyber Security Basics for Small Business" guide
- Schedule a free 45-minute consultation to discuss your specific situation - [Book time with Simon Pardo: 45 minute discovery meeting \(via Teams\)](#)

Remember: The best cyber insurance policy is one you understand and that actually works when you need it. Don't wait until after an incident to discover what's not covered.

This checklist was created based on real claim denials and coverage gaps we see in small businesses every day. Use it as a starting point but always consult with qualified professionals for your specific situation.