

Cyber insurance questionnaire worksheet

Ten security controls that small-business cyber insurance applications ask about. For each one: the question in plain words, what a true yes needs, and the evidence to have ready before anyone signs.

BUSINESS NAME

INSURANCE RENEWAL DATE

FILLED IN BY

DATE FILLED IN

IT CONTACT (PERSON OR COMPANY)

PERSON WHO WILL SIGN THE APPLICATION

HOW TO USE IT

- 1 **Fill it in early.** Sit down with whoever runs your IT before the insurer's application arrives. Evidence is easier to gather without a deadline.
- 2 **Mark Yes only when you can prove it.** Each question lists the evidence a yes needs. If a control covers only some of what the question asks, mark Partly and note the gap.
- 3 **Read the wording on the insurer's form.** On this worksheet, Yes is always the good answer. Some insurer forms ask a question the other way around, so read theirs before you copy an answer across.
- 4 **Show it to the person who signs.** Their signature says every answer is true, so they should read each answer here before it is copied onto the application.
- 5 **Keep it with the evidence.** If a claim is disputed later, the same file answers the insurer and, if it comes to that, a court.

FREE REVIEW

Free review of your renewal questionnaire.

Send us your renewal questionnaire before you submit it. We'll flag what could get you declined or overpriced, and the evidence each yes needs. There is no cost, and we reply within one business day.

Email security@obsidianridge.io with the subject "Free cyber insurance questionnaire review".

Leave out passwords, account numbers and any patient or client records. You answer and sign the application; we review the security questions.

Obsidian Ridge is not an insurance producer, broker, or agent. We do not sell, place, or advise on insurance products.

01

MULTI-FACTOR AUTHENTICATION (MFA)

Does signing in take a second step, such as a code from an app, for email, remote access, administrator and other privileged accounts, and the backup console?

MFA means a password alone does not get anyone in. Check all four places. Remote access includes VPN, RDP (Windows Remote Desktop) and remote-desktop gateways. The backup console is where the backups are managed.

YOUR ANSWER

☐**YES**☐**NO**☐**PARTLY****WHAT A TRUE YES NEEDS**

MFA is enforced in all four places, using an authenticator app or a hardware key. A shared password does not count.

EVIDENCE TO HAVE READY

- ☐ A list from your email system showing the MFA status of each user.
- ☐ The remote-access settings showing MFA on the VPN and on any RDP or remote-desktop gateway.
- ☐ A list of administrator accounts with the MFA method beside each name.
- ☐ A screenshot of the backup console showing MFA turned on.

NOTES

02

ENDPOINT DETECTION AND RESPONSE (EDR OR MDR)

Is threat-detection software installed on every computer and every server, and is someone watching its alerts around the clock?

EDR is software that detects an attack in progress on a computer. MDR (managed detection and response) is EDR with a security team watching the alerts for you. Antivirus alone is not EDR.

YOUR ANSWER

☐**YES**☐**NO**☐**PARTLY****WHAT A TRUE YES NEEDS**

EDR or MDR runs on every workstation and every server, and a named security team monitors it continuously.

EVIDENCE TO HAVE READY

- ☐ The device count from the EDR or MDR console.
- ☐ Your full device list, with workstations and servers both on it.
- ☐ The name of whoever watches the alerts around the clock.

NOTES

03

BACKUPS: OFFLINE OR IMMUTABLE, MFA-LOCKED, TESTED

Is at least one backup copy kept offline or immutable, are the backups encrypted and locked with MFA, and have you tested restoring from them in the last twelve months?

Immutable means the copy cannot be changed or deleted once it is written. A file-sync service or a shared drive does not count as a backup.

YOUR ANSWER

☐

YES

☐

NO

☐

PARTLY

WHAT A TRUE YES NEEDS

At least one copy is offline or immutable.
The backup console requires MFA, with a login kept separate from the office network.
A restore test dated within the last twelve months is on file.

EVIDENCE TO HAVE READY

- ☐ The backup settings showing the offline or immutable copy.
- ☐ The console setting showing MFA turned on.
- ☐ A dated restore-test record: what was restored, who did it, and the result.
- ☐ Confirmation that no critical backup depends on file sync alone.

NOTES

04

SECURITY TRAINING AND PHISHING TESTS

Does every employee, including anyone who handles payments, complete security awareness training at least once a year, and do you run phishing tests?

A phishing test (insurers call it a phishing simulation) is a harmless fake scam email sent to staff to see who clicks.

YOUR ANSWER

☐

YES

☐

NO

☐

PARTLY

WHAT A TRUE YES NEEDS

Every employee was trained in the last twelve months, phishing tests run on a schedule, and finance and accounts-payable staff are included.

EVIDENCE TO HAVE READY

- ☐ The training completion list, with dates.
- ☐ A dated phishing-test result, with the click-rate trend if you have it.
- ☐ A note confirming that finance and accounts-payable staff are included.

NOTES

05 WIRE AND PAYMENT-CHANGE VERIFICATION

Before sending a wire, setting up an ACH payment or changing a vendor's bank details, does someone confirm the request by calling a phone number you already had on file?

Insurers call this out-of-band verification. Replying to the email that made the request does not count, and neither does calling a number taken from it.

YOUR ANSWER

☐

YES

☐

NO

☐

PARTLY

WHAT A TRUE YES NEEDS

A written procedure requires the call for every payment change and every change to a vendor's bank details. Payments above a stated dollar amount need two people to approve them. Staff who handle payments are trained on the procedure.

EVIDENCE TO HAVE READY

- ☐ The signed call-back procedure.
- ☐ A sample from the verification log, or a ticket.
- ☐ A training record showing the finance team has read and understood the procedure.

NOTES

06 PATCHING (SECURITY UPDATES)

Do you install critical and high-severity security updates within a set number of days, with a shorter deadline for flaws that attackers are already using?

Critical and high are the two most serious ratings a security flaw can get. Most forms name thirty days. The shorter deadline covers zero-days (flaws attacked before a fix exists) and anything on CISA's Known Exploited Vulnerabilities (KEV) list, which the US government publishes.

YOUR ANSWER

☐

YES

☐

NO

☐

PARTLY

WHAT A TRUE YES NEEDS

A written patch standard states the deadline in days, and a patch report listing each device shows the standard is being met.

EVIDENCE TO HAVE READY

- ☐ The written patch standard.
- ☐ A recent patch report, listed by device, that can be matched to your device list.

NOTES

07

END-OF-LIFE SOFTWARE

Is every operating system and application still supported by its maker, with any exception either walled off from the rest of the network and the public internet, or covered by paid extended support?

End-of-life software no longer gets security fixes from its maker. Some insurer forms ask this the other way around, whether you use any end-of-life software, so read the wording before you copy your answer across.

YOUR ANSWER

☐

YES

☐

NO

☐

PARTLY

WHAT A TRUE YES NEEDS

Nothing in use is past its end-of-support date. Or every system that is past it has been segmented (walled off) and cannot be reached from the internet, or is covered by extended support.

EVIDENCE TO HAVE READY

- ☐ A list of operating systems and applications, with the support status of each.
- ☐ For any end-of-life system: a network diagram showing it is segmented and, where used, the extended-support receipt.

NOTES

08

LAPTOP ENCRYPTION

Are all laptops, and any mobile devices that hold work data, encrypted, with the recovery keys held by the company?

Encryption makes the data unreadable to anyone who finds or steals the device. On laptops, the built-in tools are BitLocker (Windows) and FileVault (Mac). A recovery key is the code that unlocks the device if the password is lost.

YOUR ANSWER

☐

YES

☐

NO

☐

PARTLY

WHAT A TRUE YES NEEDS

Every laptop is encrypted, and the company holds the recovery keys, not the individual employee.

EVIDENCE TO HAVE READY

- ☐ An encryption report covering each device.
- ☐ A note on where the recovery keys are stored and who can retrieve them.

NOTES

09

REMOTE-ACCESS TOOLS

Is every remote-access tool either unreachable from the public internet, or protected by MFA and kept behind a gateway, off its default port?

These tools let someone control a computer from somewhere else: RDP (Windows Remote Desktop), VNC, AnyDesk, TeamViewer, ScreenConnect and similar. A gateway is a checkpoint that verifies who is connecting before letting them through. Insurer forms may ask the reverse, whether remote access is exposed, so read the wording before you copy your answer across.

YOUR ANSWER

☐

YES

☐

NO

☐

PARTLY

WHAT A TRUE YES NEEDS

No remote-access tool can be reached from the internet without MFA. RDP is never left on its default port (3389) behind a password alone. Remote-support tools need someone at the computer to approve the session.

EVIDENCE TO HAVE READY

- ☐ An outside scan of what you expose to the internet, or an export of the firewall rules.
- ☐ The remote-support tool's admin settings showing MFA and on-device approval.

NOTES

10

INCIDENT RESPONSE PLAN

Do you have a written incident response plan that names who does what, and was it tested in the last twelve months?

An incident response plan is the written playbook for a cyberattack. A tabletop exercise is a meeting where the team talks through a made-up attack to test the plan.

YOUR ANSWER

☐

YES

☐

NO

☐

PARTLY

WHAT A TRUE YES NEEDS

A written plan on your firm's letterhead names who does what. A dated tabletop exercise, or a real incident, from the last twelve months shows the plan was used.

EVIDENCE TO HAVE READY

- ☐ The plan itself, or its cover page.
- ☐ The dated write-up from your last tabletop exercise.

NOTES

Your answers at a glance

Copy each answer here. For any No or Partly, write what will change, and by when.

	CONTROL	YES	NO	PARTLY	WHAT WILL CHANGE, AND BY WHEN
01	Multi-factor authentication (MFA)	☐	☐	☐	
02	Endpoint detection (EDR or MDR)	☐	☐	☐	
03	Backups	☐	☐	☐	
04	Training and phishing tests	☐	☐	☐	
05	Wire and payment-change verification	☐	☐	☐	
06	Patching	☐	☐	☐	
07	End-of-life software	☐	☐	☐	
08	Laptop encryption	☐	☐	☐	
09	Remote-access tools	☐	☐	☐	
10	Incident response plan	☐	☐	☐	

Who signs, and what the signature means

Most applications ask an executive officer to sign: an owner, a principal, a managing partner, or another officer who can legally commit the firm.

The signature says the answers are true, complete, and given after a reasonable inquiry. In practice, that means the signer has checked the security answers with whoever runs IT, and has not signed blind.

If an answer is wrong when it is signed, the insurer can rescind the policy after a loss, which means canceling it as though it had never been issued. The signature is what moves that risk from the insurer to the firm.

Before you send it back

Ten checks before the application leaves your desk. Every line should be true.

- ☐ Every question on the application is answered, with no blank fields.
- ☐ Every Yes has its evidence on file.
- ☐ Every No or Partly has a note saying what will change, and by when.
- ☐ The MFA answer covers email, remote access, administrator accounts and the backup console, not just one of them.
- ☐ The backup answer names an offline or immutable copy and a dated restore test.
- ☐ The wire-transfer answer names a written call-back procedure.
- ☐ The training answer includes finance and accounts-payable staff.
- ☐ The end-of-life software answer lists every system its maker no longer supports.
- ☐ The incident response answer names the plan and the date it was last tested.
- ☐ The person signing has read every answer before the application is filed.

READ BY (NAME OF THE PERSON SIGNING THE APPLICATION)

DATE

FREE REVIEW

Free review of your renewal questionnaire.

Send us your renewal questionnaire before you submit it. We'll flag what could get you declined or overpriced, and the evidence each yes needs. There is no cost, and we reply within one business day.

Email security@obsidianridge.io with the subject "Free cyber insurance questionnaire review".

Leave out passwords, account numbers and any patient or client records. You answer and sign the application; we review the security questions.

Obsidian Ridge is not an insurance producer, broker, or agent. We do not sell, place, or advise on insurance products.

Obsidian Ridge LLC · 964 High House Rd, PMB 2086, Cary, NC 27513
(984) 999-7785 · security@obsidianridge.io · obsidianridge.io