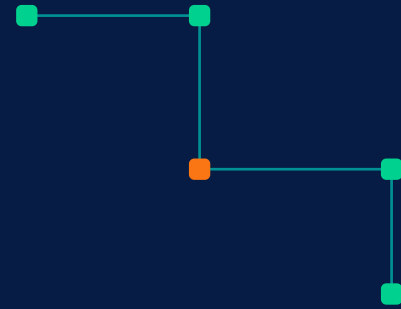


Cyber Insurance Application Readiness Checklist.



Your renewal application is a signed representation. If an answer doesn't match what an investigator finds after an incident, the carrier can deny the claim or rescind the policy. Use this checklist to confirm each answer is true across your whole environment, and to build the evidence file before you sign.

How to use it

- 1 Assign the roles.**
Finance owns the signature. IT or your MSP owns the evidence. They shouldn't be the same person.
- 2 Work the controls.**
Tick an item only when the evidence exists and covers every account, device or system in scope.
- 3 Write down the exceptions.**
Where the honest answer is "mostly," disclose the gap on the application.
- 4 Review the policy terms.**
Check limits, retentions and sublimits against your own downtime and fraud exposure.

Renewal details

Company	
Renewal date	
Carrier / broker	
Signer (finance)	
Evidence owner (IT / MSP)	
Checklist started	

What a wrong answer can cost

Worked example from the article, using illustrative assumptions. Replace the example column with your own figures.

	Example company (assumption)	Your company
Annual revenue / employees	\$25,000,000 / 120	
Five-day outage: lost revenue + idle payroll	\$457,360	
Policy limit	\$1,000,000	
Retention	\$25,000	
Funds transfer fraud sublimit	\$100,000	
Funds transfer fraud loss (Coalition 2025 average)	\$141,000	
You pay if the application is accurate	\$25,000 retention (outage); \$41,000 over sublimit (fraud)	
You pay if the policy is rescinded	Everything: \$457,360+ (outage); \$141,000 (fraud)	

Outage figure from Xceptional's downtime worked example (\$100,000/day revenue, \$54.00/hr loaded labor). Policy terms are illustrative assumptions, not a quote or benchmark. Coverage is also subject to the policy's business interruption terms and waiting period. Run your own numbers in the Downtime Cost Calculator.

1. Identity and MFA

MFA scope is the question most often misstated. "We have MFA" usually means email. The form usually asks about more.

A defensible "yes" means	Evidence to keep on file	Owner / date pulled
☐ MFA enforced for every user's email, with no legacy sign-in methods left open	Identity provider enforcement report by user; list of any excluded accounts	
☐ MFA on VPN and every other remote access path	Remote access configuration showing MFA required	
☐ MFA on every admin and privileged account, including service desk and break-glass accounts	Privileged account list with MFA status for each	
☐ MFA on cloud admin consoles (Microsoft 365, Google Workspace, Azure, AWS)	Screenshot of admin MFA or conditional access policy	
☐ MFA on the backup system console	Backup platform security settings	
☐ Vendor and MSP access requires MFA and is logged	Vendor access list with MFA status and log location	
☐ Phishing-resistant MFA for admins and executives, if the form asks	Enrolled methods report (FIDO2 keys, passkeys)	

2. Endpoints and servers

A defensible "yes" means	Evidence to keep on file	Owner / date pulled
☐ EDR on every workstation, laptop and server, matched to the asset inventory	EDR console export reconciled to inventory; gap list with dates	
☐ Alerts monitored and answered 24/7, internally or through an MDR provider	MDR contract or on-call schedule; sample alert response	
☐ Unsupported operating systems and software identified, including shop-floor and lab PCs	Unsupported asset list with isolation or other compensating controls	
☐ Local admin rights removed from standard users	Group policy or endpoint management report	

3. Backups and recovery

A defensible "yes" means	Evidence to keep on file	Owner / date pulled
☐ At least one backup copy is offline or immutable	Backup configuration showing immutability or air gap	
☐ Backup credentials are separate from the main domain and protected by MFA	Backup account list and authentication settings	
☐ A full restore was tested within the carrier's stated window	Restore test record with date, system restored and time taken	
☐ Recovery time for critical systems is documented and realistic	Recovery objectives by system, compared to the last test	

4. Patching and exposure

A defensible "yes" means	Evidence to keep on file	Owner / date pulled
☐ A written patch window exists for critical vulnerabilities	Patch policy with the stated window	
☐ Internet-facing systems meet that window	Patch compliance report for the last 90 days	
☐ Remote desktop is not exposed directly to the internet	External port scan or firewall rule review	
☐ You've scanned your own external footprint and fixed findings before submitting	External scan report with remediation notes	

5. Email and payments

Business email compromise and funds transfer fraud made up 58% of Coalition's 2025 claims. These controls are often asked about separately from the rest.

A defensible "yes" means	Evidence to keep on file	Owner / date pulled
☐ Email filtering plus SPF, DKIM and DMARC on your domains	Email security settings; DMARC record and policy level	
☐ Callback verification on a known number for any bank detail change	Written payment procedure; sample of completed callbacks	
☐ Dual approval for wires above a set amount	Bank or ERP approval settings	
☐ You know your funds transfer fraud and social engineering sublimit	Policy declarations page with sublimit noted	

6. Incident response and training

A defensible "yes" means	Evidence to keep on file	Owner / date pulled
☐ A written incident response plan with names, phone numbers and the carrier's hotline	Current plan with revision date	
☐ The plan names the carrier's required panel vendors, if any	Policy panel requirements compared with the plan	
☐ A tabletop exercise in the last 12 months	Exercise date, attendees and follow-up actions	
☐ Security awareness training and phishing tests for all staff	Completion rate and most recent phishing test results	

7. Before you sign

A defensible "yes" means	Evidence to keep on file	Owner / date pulled
☐ Every "yes" has an evidence file entry dated within the last 30 days	Evidence file index	
☐ Every exception is written into the application or a cover letter	Copy of disclosures sent to the broker	
☐ Limits compared against your downtime and fraud exposure	Downtime Cost Calculator output; the example table on page 1	
☐ Retention, waiting period, sublimits and key exclusions reviewed with your broker	Broker notes or email	
☐ Last year's application compared against this year's answers	Marked-up prior application	

90-day renewal timeline

A suggested schedule, counted back from the renewal date. Adjust it to your broker's submission deadline.

Days before renewal	Milestone	Target date
90	Kickoff. Assign signer and evidence owner. Pull last year's application and this year's questionnaire.	
75	Collect evidence for sections 1 through 6. Log every gap.	
60	Close the gaps you can. Document compensating controls for the rest.	
45	Draft answers. Write up exceptions.	
30	Broker review. Negotiate limits, retentions and sublimits.	
14	Final evidence refresh. Signer reviews the evidence file.	
0	Sign and submit. File the evidence with the signed application.	

Sign-off

Both signatures confirm that each answer on the application has matching evidence on file and that every known exception was disclosed.

Finance (application signer)	IT / MSP (evidence owner)
Name	Name
Title	Title
Date	Date

Want a second set of eyes before you sign?

We'll walk your answers against the evidence and flag anything that wouldn't hold up.

xceptional.com/contact →



Sources. Coalition 2026 Cyber Claims Report press release (Mar. 5, 2026). Lockton, Travelers v. ICS analysis (Sept. 15, 2022). Questions vary by carrier. Example figures are illustrative assumptions.