

Cyber Insurance Renewal Readiness Checklist

Work through this before your next cyber insurance renewal so every answer on the application matches what is actually in place, with evidence to prove it. Requirements vary by carrier and policy; confirm with your broker.

Renewal timeline

When	What to do
About 90 days out	Get last year's application and this year's form from your broker. Name an internal owner.
About 60 days out	Run a readiness review: compare every answer to what is actually deployed. List the gaps.
About 30 days out	Close the quick gaps, document the rest with dates, and assemble the evidence pack.
At submission	Answer from evidence, not memory. Keep a copy of every answer and attachment.

Control checklist

Done	Control	What applications commonly ask	Evidence to gather
☐	MFA	Email, remote access, admin accounts and cloud apps all require MFA?	Screenshot or export of MFA enforcement and exceptions
☐	Endpoint protection	EDR on every server and workstation, monitored 24/7?	Device count vs protected count; monitoring terms
☐	Backups	Copies kept separate from production and restores tested?	Backup scope, separation method, last restore test
☐	Patching	Critical updates applied on a defined schedule?	Patch policy and a recent compliance report
☐	Email and training	Filtering, SPF, DKIM, DMARC, phishing simulation and training?	DMARC status, training completion records
☐	Privileged access	Admin rights limited and reviewed?	List of admin accounts and last review date
☐	Remote access	No remote desktop open to the internet; VPN or SASE with MFA?	External scan result and remote access method
☐	Incident response	Written plan, tested with leadership?	IR plan and most recent tabletop summary
☐	Policies	Written information security program (WISP)?	Current WISP with approval date
☐	Vendors	Vendor and installer remote access controlled and logged?	Vendor access list and method
☐	Logging	Security logs kept long enough to investigate?	Log sources and retention period

Build your evidence pack

- ☐ Completed application with the evidence behind each answer
- ☐ Network and device inventory
- ☐ MFA, EDR and backup reports from the last 30 days
- ☐ Recent vulnerability scan or penetration test report
- ☐ Current WISP and incident response plan
- ☐ Training and phishing simulation records
- ☐ Tabletop exercise summary
- ☐ Carrier hotline and policy number, stored offline

Common renewal mistakes

- Answering "yes" to MFA when some accounts or apps are exempt
- Counting antivirus as EDR
- Backups on the same network, with the same admin passwords, as production
- An incident response plan that no one has read or tested
- Different answers on different forms from year to year

If you have an incident

- Follow your policy: contact your carrier's claims or breach hotline before hiring outside firms
- Preserve evidence; do not wipe systems first
- Work your incident response plan and keep a written timeline

Assign owners and dates

Gap found	Owner	Due	Done
			☐
			☐
			☐
			☐
			☐
			☐

Questions for your IT or security provider before renewal

- ☐ Can you export MFA, EDR and backup status for every user and device?
- ☐ Which application answers would you change today, and why?
- ☐ When was our incident response plan last tested, and who attended?
- ☐ Who will coordinate with our carrier and its designated response team during a claim?

BTI in Chicagoland: office in Downers Grove with BTI staff on site across Chicagoland. BTI does not sell insurance or give coverage advice. BTI works with your carrier's requirements, builds them into your WISP, incident response plan, policies and evidence controls, and during an incident coordinates with your carrier and its designated response team.

Book a free consultation
btigroup.com/freeconsultation/

Chicagoland IT team: 312-492-2613

BTI Communications Group: over 40 years in business technology, a 24/7 NOC/SOC, and ISO 27001 compliant policies and controls. This checklist is general guidance, not legal or insurance advice.