



10 Tips to Complete Your Cyber Insurance Application

1. Start Early and Designate One Primary Owner

Begin the application process 2-4 months before renewal. Assign one person (IT manager, CISO, CFO, or other relevant employee) to complete the entire application using available information, then have your MSP review only the technical sections for accuracy.

2. Be Accurate with Revenue Information

Premium calculations are based on your revenue figures. Use exact numbers from audited financial statements and include all entities covered under the policy. This directly impacts your cost, so precision matters.

3. Check "Yes" for Planned Implementations

If you're planning to implement a security control, check "Yes" and specify the planned date. For example: "MFA implementation scheduled for Q2 2025" or "Endpoint encryption rollout planned for March 2025."

4. Provide Data Record Estimates When Exact Numbers Aren't Available

For PII, PHI, PCI, and biometric data counts, use reasonable ranges:

- Small business: "1,000-5,000 records"
- Medium business: "5,000-25,000 records"
- Large operations: "25,000-100,000+ records"

5. Create an MFA Implementation Appendix

List all systems and their multi-factor authentication status:

- **Systems WITH MFA:** Email, cloud applications, VPN, backup systems
- **Systems WITHOUT MFA:** Legacy applications, local servers
- **Planned MFA rollouts** with target implementation dates

6. Specify Security Vendors Not in Dropdown Menus

When your security provider isn't listed, write in the specific vendor:

- **EDR/NGAV:** CrowdStrike, SentinelOne, Microsoft Defender
- **Email Security:** Proofpoint, Mimecast
- **Backup Solutions:** Veeam, Acronis, Carbonite



7. Choose the Right Cybersecurity Contact

This is who would be the go-to liaison between the insurance company and your company if there is a security incident

Designate your cybersecurity contact (list more than one in an appendix if needed):

1. Internal CISO or Chief Security Officer
2. Head of IT or CTO
3. External MSP security lead
4. Risk manager or equivalent

8. Be Completely Honest About Prior Incidents

Transparency about past incidents within the 3-year lookback period is crucial. Report all unauthorized network activity, data breaches, system outages over 6 hours, and social engineering attacks. Hiding incidents is the #1 cause of claim denials.

9. Document Backup and Recovery Capabilities

Clearly specify your backup arrangements:

- **Frequency:** Daily, weekly schedules
- **Type:** Cloud-based, on-premises, or hybrid
- **Segmentation:** Note if backups are air-gapped or offline
- **Testing:** Include annual restoration testing

10. Have Authorized Signatory Complete and Review

The application must be signed by CEO, President, CIO, CTO, CSO, COO, CFO, General Counsel, or Risk Manager. Ensure this person reviews the completed application and understands they're certifying its accuracy under penalty of insurance fraud laws.

Remember: Accuracy over perfection - insurers prefer honest organizations with clear security roadmaps over those claiming perfect implementation without evidence.

BONUS: Communicate with your cyber insurance agent if you have any questions. The agent is there to help you through the cyber insurance buying experience.

Contact [Joe Erle](mailto:JoeErle@c3insurance.com) at C3 Insurance: Joe@c3insurance.com or 805-305-0377