Coalition®

techRisks.com
A Technology Service Organization.

Return Via E-Contact@Techrisks.com
to assess your Networks and stay on top of your
Cyber Risks Exposures with Active Monitoring
Question? Toll: 866.355.RISK (7475)

Questions for Cyber Insurance

Responses to the questions below are necessary to obtain a quotation for Cyber insurance from Attestation Questions must be completed. After a quotation for insurance is bound, the Named Insured will be asked to electronically sign an application populated with the responses from the questions below.

NAMED INSURED

WEBSITE DOMAIN(S)

PRIMARY INSURED EMAIL CONTACT	SECURITY/IT EMAIL CONTACT		
ADDRESS	**CITY**	**STATE**	**ZIP**
INDUSTRY	**NO. OF EMPLOYEES**	**REVENUE*** $	**GROSS PROFIT / NET REVENUE*** $

* Next 12 months

Attestation Questions

1 Within the last 3 years has *Named Insured* suffered any cyber incidents resulting in a claim in excess of $25,000?   NO   YES

(If Yes) please explain the cyber incidents and/or claims.

2 Is *Named Insured* aware of any circumstances that could give rise to a claim under this insurance policy?   NO   YES

(If Yes) please explain the circumstances and/or potential claims.

3 Does *Named Insured* implement encryption on laptop computers, desktop computers, and other portable media devices?   NO   YES   SOMETIMES

4 Does *Named Insured* collect, process, store, transmit, or have access to any Payment Card Information (PCI), Personally Identifiable Information (PII), or Protected Health Information (PHI) other than employees of *Named Insured*?   NO   YES

4a (If Yes) What is the estimated annual volume of payment card transactions (credit cards, debit cards, etc.)?

NO RECORDS   LESS THAN 100,000   100,000 – 500,000   500,000 – 1,000,000   OVER 1,000,000:

4b (If Yes) How many PII or PHI records does *Named Insured* collect, process, store, transmit, or have access to?

NO RECORDS   LESS THAN 100,000   100,000 – 500,000   500,000 – 1,000,000   OVER 1,000,000:

5 For which of the following services do you enforce Multi-Factor Authentication (MFA)?

5a Email   NO   YES

5b Virtual Private Network (VPN), Remote Desktop Protocol (RDP), RDWeb, RD Gateway, or other remote access   NO   YES   N/A

5c Network/cloud administration or other privileged user accounts   NO   YES   ON ADMINISTRATIVE ACCOUNTS AND ALL CLOUD SERVICES WHERE SUPPORTED

Attestation Questions (continued)

		NO	YES	N/A
6	Does *Named Insured* maintain at least weekly backups of all sensitive or otherwise critical data and all critical business systems offline or on a separate network?	NO	YES	N/A
7	Does *Named Insured* require a secondary means of communication to validate the authenticity of funds transfers (ACH, wire, etc.) requests before processing a request in excess of $25,000?	NO	YES	N/A
8	Within the last 3 years has *Named Insured* been subject to any complaints concerning the content of its website, advertising materials, social media, or other publications?	NO	YES	N/A
9	Does *Named Insured* enforce procedures to remove content (including third party content) that may infringe or violate any intellectual property or privacy right?	NO	YES	N/A

Optional: Which of the following IT security controls does the applicant have in place?

	NO	YES	N/A
Anti-virus and Firewalls (Windows 10 or higher qualifies for <10 employees)	NO	YES	N/A
Encryption of Sensitive Data at Rest and In Transit	NO	YES	N/A
Encryption and Endpoint Protection on Mobile Computing Devices	NO	YES	N/A
Formal Vulnerability Management and Software Patching Procedures	NO	YES	N/A
Formal Data Backup and Recovery Procedures in Place and Tested Periodically	NO	YES	N/A
Formal Cyber Incident Response Plan in Place and Tested Periodically *if they don't have one, TechRISKS.com amd MSP can provide one complimentary upon binding.*	NO	YES	N/A
Does the Applicant rely on Cloud Computing, Software-as-a-Service, or any other outsourced computer hosting for revenue-generating operations?	NO	YES	N/A
Does the applicant deal with protected health information as defined by HIPAA?	NO	YES	N/A

How did you hear about us? Your MSP?   Additional Questions?