Cyber Insurance Questionnaire

Tell us about your business

Company name	
Primary Business Address	
Primary Website URL	
□ I acknowledge that the customer does not have a website	
Estimated annual revenue (next 12 months)	**Estimated annual revenue is the same as last fiscal year's revenue**: □Yes □No, last fiscal year's revenue was $____________________
How many employees does your business have?	
NAICS code/Business Description:	
□ **Company does NOT operate in any of the following:** Adult Content, Cannabis, Cryptocurrency or Blockchain, Gambling, Payment Processing (e.g. as a payment processor, merchant acquirer, or Point of Sale system vendor), Debt collection agency, Managed IT service provider (MSP or MSSP). We are unable to quote thse types of businesses at this time.	

Cyber Liability

Policy Period | **Effective Date:** ____________________ **Expiration Date:** ____________________

Within the last five years, has the applicant experienced any claim, loss, breach, or event of any type that could give rise to a claim, that could fall in the scope of a cyber liability policy?

□ Yes
□ No

If you answered Yes:

Within the last five years, has the applicant experienced any claim that could fall in the scope of a cyber liability policy?

□ Yes □ No

Total claim amount: ____

When did claim occur? ____

Is the applicant aware of any of the following? *(Select all that apply)*

□ Fact, circumstance, situation or event that could potentially give rise to a claim
□ Media complaint
□ Regulatory or legal action
 □ Action still open?
 □ Action closed with fines?
□ Network Instrusion, Denial of service attack, or unauthorized loss of information
□ Unscheduled network outage

Additional comments:

Provide details of the incident (such as how and when it occurred), and if any steps have been taken to mitigate future losses.

Does the applicant user Multi-Factor Authentication (MFA)?

Check all that apply:

□ Remote email access
□ Remote network access
□ Remote email access not allowed
□ Remote network access not allowed
□ Administrator/privileged user accounts (all)
□ Administrator/privileged user accounts (where allowed)

Does the applicant store or process personal, health, or credit card information?

□ Yes
□ No

How many PII and PHI records does the applicant store or process?

(Check all that apply)

□ None
□ <100k
□ 100k-250k
□ 250k-500k
□ 500k-1m
□ 1m-2.5m
□ 2.5m-5m
□ 5m-10m
□ +10m
□ No records are biometric

How many PCI records does the applicant store or process?

(Check all that apply)

□ None
□ <100k
□ 100k-250k
□ 250k-500k
□ 500k-1m
□ 1m-2.5m
□ 2.5m-5m
□ 5m-10m
□ +10m
□ Total number of records stored or processed are below 1m

Does the applicant backup all sensitive information?

□ Yes
□ No

If you answered Yes:

What frequency does the applicant backup?

□ Continuously
□ Daily
□ Weekly
□ Monthly
□ Less than Monthly

Describe the characteristics of the applicant’s backups?

(Select all that apply)

□ Offline air-gapped
□ Cloud-based
□ MFA Protected
□ Encrypted
□ Tested
□ Recoverable within 3 days

Which security procedures and controls does the applicant use?

Better security procedures and controls may improve pricing,coverage and the number of quotes received.

Payment & Transfers Controls *(Check all that apply)*

□ Requires prior verification by at least 2 employees over $25k
□ Requires a secondary means of communication to validate authenticity over $25k
□ Has transfer controls in place for below $25k
□ Fully outsource payment card processing
□ Payment card processing is PCI compliant
□ Deploys either end-to-end or point-to-point encryption technology

Security *(Check all that apply)*

□ Encrypts all sensitive information on all devices
□ Provide mandatory information security training
□ Enforces procedures to remove content that may infringe or violate any intellectual property or privacy right
□ Installs all firewall, patches, anti-virus, anti-spyware updates and patches within 30 days.
□ Uses an email security filtering tool
□ Uses an Endpoint Detection and Response (EDR) product

Cyber Liability Supplemental Questions

Required for Tokio Marine HCC only:

Which Multi-factor Authentication (MFA) provider does the applicant use? ______________________________

Which Firewall provider does the applicant use? ______________________________

Which email security filtering provider does the applicant use? ______________________________

Which Endpoint Detection and Response (EDR) provider does the applicant use? ______________________________

Required for Cowbell P250 only:

How often does the organization apply updates to critical IT-systems and applications? (optional)

☐ Weekly
☐ Monthly
☐ Quarterly
☐ Every 6 Months
☐ Never

Does the organization have an incident response plan - tested and in-effect - setting forth specific action items and responsibilities for relevant parties in the event of cyber incident or data breach matter? (optional)

☐ Yes
☐ No

Are all internet-accessible systems (e.g. web-, email-servers) segrafated from the organization's trusted network (e.g. within a demilitarized zone (DMZ) or at a third-party serice provider)? (optional)

☐ Yes
☐ No

Do agreements with third-party service providers require levels of security commensurate with the organization's information security standard? (optional)

☐ Yes
☐ No