

Cyber Liability Questionnaire

Account Information

Business Name

Primary Business Address

Primary Website Address

I acknowledge this business does NOT have a website.

Estimated annual revenue (next 12 months)

Estimated annual revenue is the same as last year's revenue.

Annual revenue (last fiscal year)

How many employees does your business have?

NAICS Code - What is the main type of work your company does?

Company does NOT operate in any of the following: Adult Content, Cannabis, Opioid Manufacturing, 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) or Health Information Exchange.

Policy Period

Effective Date

Expiration Date

Cyber Liability

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

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

- \$0
- \$1 - \$10K
- \$10K - \$25K
- \$25K - \$50K
- \$50K - \$100K
- \$100K - \$250K
- \$250K - \$500K
- \$500K+

Enter total claim amount

When did claim occur?

- Within the past 3 years
- Within the past 5 years

How many claims in total?

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

- Network intrusion, denial of service, or unauthorized loss of information

- Media complaint
- Regulatory or legal action
- Unscheduled network outage
- Fact, circumstance, situation or event that could potentially give rise to a claim
- Actual or attempted extortion demand with respect to its computer systems
- Notified customers or any other third party of a data breach incident

Is the regulatory or legal action still open?

- Open
- Closed with fines
- Closed without fines

Additional Comments

Where does the applicant enforce multi-factor authentication (MFA) or not allow remote access? (Select all that apply)

- Remote email access
- Remote email access not allowed
- Remote Network/Virtual Private Network (VPN) access
- Remote Network/Virtual Private Network (VPN) 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 of more than 500k individuals?

- Yes
- No

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

- No records
- 1-100k

- 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?

- No records
- 1-500
- 500-100k
- 100k-250k
- 250k-500k
- 500k-1m
- 1m-2.5m
- 2.5m-5m
- 5m-10m
- +10m

Total number of records stored or processed is below \$1m

Does the applicant backup all sensitive/critical information?

- Yes
- No

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? (Select all that apply)

Payment & Transfer Controls

- Requires prior verification by at least two employees for transfers over \$25k
- Requires a secondary means of communication to validate authenticity for transfers over \$25k, and change banking details
- Has transfer controls in place for prior verification and secondary means of communication for amounts below \$25k, and for any change in banking details
- Fully outsourced payment card processing
- Payment card processing is PCI compliant
- Deploys either end-to-end or point-to-point encryption technology

Security Procedures

- Encrypts all sensitive information on all devices
- Provides mandatory information security training inclusive of social engineering training
- 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
- Has an active technology errors and omissions policy concurrent with this insurance policy
- Enforces procedures to review/remove content that may infringe or violate any intellectual property or privacy right
- Has an incident response plan, Business Continuity Plan or Disaster Recovery 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
- All internet-accessible systems (e.g. web-, email-servers) segregated from the organization's trusted network (e.g. within a demilitarized zone (DMZ) or at a third-party service provider)

Agreements with third-party service providers require levels of security commensurate with the organization's information security standard

Beazley - Supplemental Questions

These questions are not mandatory, but will help get more accurate quotes.

Has the company, within the past 12 months, completed or agreed to, or do you contemplate entering into within the next 12 months, a merger, acquisition, or consolidation?

- Yes
- No

Does the company have any revenue-generating operations outside of the US?

- Yes
- No

Percentage of revenue generated outside of the US

Cowbell Prime 250 - Supplemental Questions

These questions are only required for Cowbell Prime 250.

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

- Weekly
- Monthly
- Quarterly
- Every 6 months
- Never

Security Provider - Supplemental Questions

These questions are only required for At-Bay (Non-Admitted) & Tokio Marine - HCC (Non-Admitted)

Please select the MFA Provider

- Auth0
- Duo
- LastPass

- Okta
- OneLogin
- Other
- Unknown

Which of the following Inbound Email Security products (i.e. Secure Email Gateway (SEG)) products does the applicant use, if any?

- Avanan
- Barracuda
- Cisco
- Microsoft Defender
- Mimecast
- Proofpoint
- SonicWall
- Symantec
- Trend
- Micro
- Apprivo
- Darktrace
- Datto
- Google
- Inky
- Intermedia
- Ironscales
- Perception Point
- Other
- Unknown

Which of the following Endpoint Detection & Response (EDR) products does the applicant use, if any?

- BitDefender
- Carbon Black Cloud
- Cisco AMP

- CrowdStrike Falcon Endpoint Protection
- Cybereason Defense Platform
- Cynet360
- Endgame Endpoint Protection
- FireEye Endpoint Security
- Fortinet FortiEDR
- Malwarebytes Endpoint Protection and Response
- McAfee MVision EDR
- RedCanary
- RSA Netwitness
- SentinelOne
- SolarWinds
- Sophos Intercept X
- Symantec EDR Symantec Endpoint Security (SES) Complete
- Windows Defender Endpoint
- Cycraft XSensor
- IBM Security QRadar EDR
- Microsoft Defender for Endpoint (E5)
- Palo Alto Networks Cortex XDR
- Trellix Endpoint Detection and Response (EDR)
- Other
- Unknown

Do you use a next-generation antivirus (NGAV) product to protect all endpoints across your enterprise?

- Yes
- No

Please specify the NGAV Provider

- BitDefender
- Carbon Black
- Check Point Software Technologies

- Cisco AMP
- CrowdStrike
- Cylance
- ESET
- Fortinet
- F-Secure
- Kaspersky
- Malwarebytes
- McAfee
- Microsoft
- Palo Alto Networks
- Panda Security
- SentinelOne
- Sophos Intercept
- Symantec
- TrendMicro
- Windows Defender Endpoint
- Other
- Unknown