SAYATA

CYBER INSURANCE QUOTE

City of Powder Springs

Cost and coverage may change based on final responses submitted in the application.

QUOTE EXPIRATION DATE
04/10/2022

COWBELL CYBER™

All information in this document was created by the insurer, and policy prices does not entail taxes & fees

COWBELL CYBER

support@cowbellcyber.ai cowbell.insure

CYBER COVERAGE WITH CLOSED LOOP RISK MANAGEMENT

Get peace of mind with a Cowbell cyber insurance policy. Cowbell Prime is Cowbell's standalone, admitted cyber insurance program. Our policies are written on AM Best "A" or "A-" rated papers and backed by top global reinsurers.

CYBER INSURANCE MADE EASY

A pioneer in cyber insurance, Cowbell innovates to make cyber insurance easy and brings clarity to cyber coverage for organizations like yours:

- Get limits and coverages dedicated solely to cyber events
- Get coverage for multiple categories of cyber threats – not just data breaches
- Cowbell cyber policies are not "one size fits all" – they are matched to your needs and unique risk exposure

THE UNIQUE COWBELL APPROACH

Gain complete insight into your organization's risk exposure using Cowbell Cyber's early warning system. From risk discovery to remediation, our AI-powered risk resources help you improve your risk profile.

Cowbell Cyber Insurance Quote - Prime 100

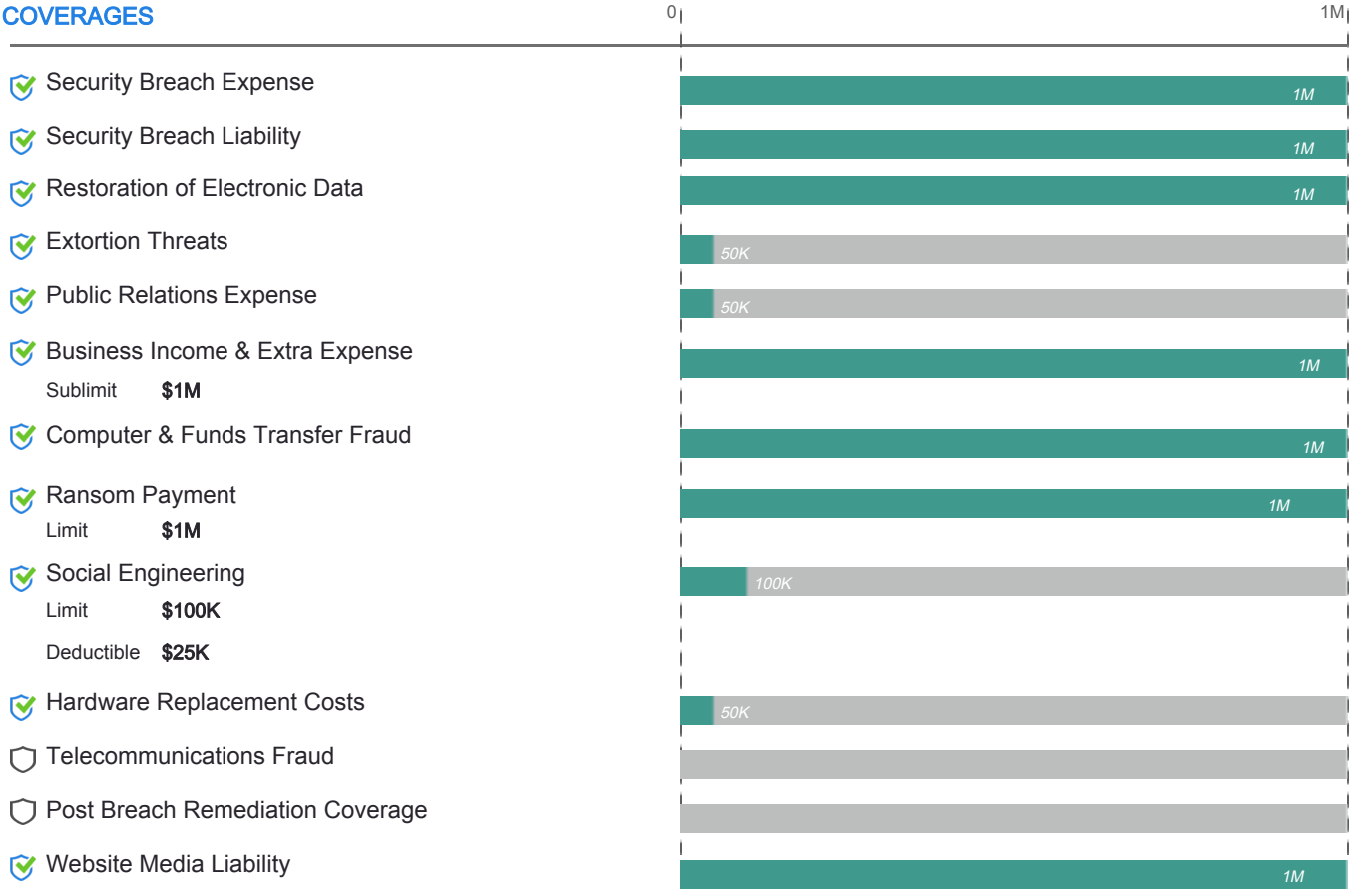
NAMED INSURED	**City of Powder Springs**	AGENCY NAME	**Sayata Labs**
REVENUE	**$17,014,583.00**	QUOTE NUMBER	**QCB-100-VC1UYLUI**
# OF EMPLOYEES	**50**		
YEAR ESTABLISHED	**2020**	EXPIRES ON	**2022-04-10 (12:01 AM)** Insured Local Time
INSURED STATE	**GA**		

Thank you for trusting Cowbell for your cyber coverage. Below is the detail of your quoted cyber policy based on the truthfulness and accuracy of the information provided to Cowbell in response to the questions on the insurance application entered into our underwriting system. After quote expiration date, underwriters generally reserve the right to revise the offered quotes. All quotes are subject to signed Cowbell application and confirmation of loss history.

PROPOSED POLICY DETAILS

AGGREGATE LIMIT	**$1,000,000**	POLICY PERIOD	**04/02/2022 to 04/02/2023**
DEDUCTIBLE	**$25,000**	ESTIMATED ANNUAL PREMIUM	**$2,739.00**
		Processing Fee	$195.00
WAITING PERIOD	**6 Hrs**	BROKER FEES	**$100.00**
RETROACTIVE PERIOD	**Full Prior Acts**	TOTAL AMOUNT	**$3,034.00**

COVERAGES



COWBELL™ CYBER

Cowbell Factors™

We included below your Cowbell Factors rating which gives you visibility into your security posture, how you compare to peers, and where to improve your security. Cowbell's platform assesses your threats and risk exposure using Cowbell Factors and automatically tailors the coverage offered to your specific business needs. Scores range from 0 to 100, 100 being the highest and representing the lowest level of risk.

AGGREGATE COWBELL FACTORS

COMPANY AGGREGATE

City of Powder Springs

Average of all the various Cowbell Factors for this company. This score ranges from 0 to 100, 100 being the highest. A company with a score of 85 represents less risk than one with a score of 64. This ACF is a good metric to benchmark a company against peers, but it is not used for underwriting.

INDUSTRY AGGREGATE (921110)

Public Administration, Executive Offi

Measures an industry overall cyber risk factor. This is calculated from the pool of organizations in the Cowbell database for the specific industry. This score ranges from 0 to 100, 100 being the best. An industry with a score of 80 represents less risk than one with a score of 56.

INDIVIDUAL COWBELL FACTORS

NETWORK SECURITY

Measures the strength of the organization's network infrastructure and whether security best practices are deployed such as use of encryption, secure protocols, patching frequency, and use of threat mitigation tools. This factor also checks for vulnerabilities, malware, misconfigurations and other weaknesses.

FUNDS TRANSFER

This factor tracks risk markers related to hacking of email and phishing that commonly leads to nefarious activities such as funds transfer.

CLOUD SECURITY

Measures the strength of an organization's cloud security based on its security practices and footprint on commonly used public clouds and cloud storage (i.e. AWS, Azure, GCP, Box). This factor incorporates configuration for security best practices such as the use of multi-factor authentication.

CYBER EXTORTION

Measure of an organization's potential exposure to extortion related attacks such as ransomware. This factor shares some data sources with network security and endpoint security presence of malware on the network, patching cadence, use of encryption and more.

ENDPOINT SECURITY

Measure of endpoints preparedness (servers, mobile devices, IoT endpoints) towards cyberattacks. This factor incorporates the number of endpoints as well as the level of security hygiene applied to them - patching cadence and presence of vulnerabilities or malware.

COMPLIANCE

Measures an organization's level of compliance to security standards such as CIS (Center of Internet Security) benchmarks, NIST CSF (Cyber Security Framework), CSC-20 (Critical Security Controls), HIPAA, PCI, EU GDPR and CCPA (future).

DARK INTELLIGENCE

Measure of an organization's exposure to the darknet, taking into account the type and volume of data exposed and its value for criminal activity (examples: stolen credentials, PII).

Cowbell Cyber Coverages - Prime 100

SECURITY BREACH EXPENSE

Coverage for losses and expenses directly associated with recovery activities in the aftermath of a cyber incident. This can include investigation and forensic services, notification to customers, call center services, overtime salaries, post-event monitoring services such as credit monitoring for impacted customers and more.

SECURITY BREACH LIABILITY

Coverage for third party liability directly due to a cyber incident and that the insured becomes legally obligated to pay. This includes defense expenses, compensatory damages, and settlement amounts, and fines or penalties assessed against the insured by a regulatory agency or government entity, or for non-compliance with the Payment Card Industry Data Security Standards.

RESTORATION OF ELECTRONIC DATA

Coverage for the costs to replace or restore electronic data or computer programs in the aftermath of an incident. This can also include the cost of data entry, reprogramming and computer consultation services to restore lost assets.

EXTORTION THREATS

Coverage for loss resulting from an extortion threat that is discovered during the policy period. This can include approved firms and resources that determine the validity and severity of threat, interest costs associated with borrowing for the ransom demand, reward payment that leads to conviction and arrest of party responsible, the ransom payment and other reasonable expenses.

PUBLIC RELATIONS EXPENSE

Coverage for the fees and costs to restore reputation in response to negative publicity following a cyber incident or a security breach. This includes, for example, the fees associated with the hiring of a public relations firm that handles external communications related to the breach.

COMPUTER AND FUNDS TRANSFER FRAUD

Coverage for the losses due to a fraudulent computer operation that causes money (or other property) to be transferred from an insured's account. This also covers losses incurred by a fraudulent instruction directing a financial institution to debit money from the insured's transfer account.

BUSINESS INCOME AND EXTRA EXPENSE

Coverage for the losses and costs associated with the inability to conduct business due to a cyber incident or an extortion threat. Business income includes net income that would have been earned or incurred. Note that business interruptions due to system failure or voluntary shutdown are not covered.

SOCIAL ENGINEERING

Coverage for a loss resulting from a social engineering incident where the insured is intentionally misled to transfer money to a person, place or account directly from good faith reliance upon an instruction transmitted via email by an imposter. A documented verification procedure requirement needs to have been completed in order to be provided coverage.

RANSOM PAYMENTS

Coverage for the reimbursement of the monetary value of any ransom payment made by the insured to a third party in response to a ransom demand to resolve an extortion threat.

HARDWARE REPLACEMENT COSTS

Coverage for the cost to replace computers or any associated devices or equipment operated by the insured that are unable to function as intended due to corruption or destruction of software or firmware, resulting from a cyber incident.

TELECOMMUNICATIONS FRAUD

Coverage for the cost of unauthorized calls or unauthorized use of the insured's telephone system's bandwidth, including but not limited to phone bills.

POST BREACH REMEDIATION COVERAGE

Coverage for labor costs incurred to resolve vulnerabilities or weaknesses in the insured's computer system that are identified by an independent security firm after a cyber incident. Identified upgrades or improvements must reduce the probability or potential damage of a future incident to qualify.

WEBSITE MEDIA LIABILITY

Coverage for a loss and defense expenses from intellectual property infringement, other than patent infringement, related to media content on the company website or its social media accounts only.