CYBER INSURANCE QUOTE PROPOSAL
PRIME 100

CYBER INSURANCE MADE EASY

Cowbell gives you peace of mind with standalone cyber coverage tailored to your unique needs. Our Prime 100 cyber insurance policies are designed to cover today's and tomorrow's threats, backed by top reinsurers, and packaged with robust risk engineering services.

CLOSED-LOOP RISK MANAGEMENT

Our unique approach enables you to continuously improve your risk profile and stay ahead of threats.

ASSESS

Cowbell Factors®, our risk ratings, compare your business' risk profile to your industry peers.

RESPOND

Cowbell's cyber experts are on-call 24×7 to help you recover quickly from cyber incidents.

INSURE

The quote below is custom-designed to suit your cyber risk profile and your needs.

IMPROVE

Our risk engineers help proactively mitigate risk and improve your security standing with continuous risk monitoring and advice.

CONTINUOUSLY IMPROVE YOUR RISK PROFILE

Take advantage of the resources available with your policy:

- Use our Incident Response Plan template to get prepared
- Identify security partners on **Cowbell Rx** to strengthen your security
- Deploy a cyber awareness training program to all your employees - 20 seats are included with our training partner, Wizer

CYBER INSURANCE QUOTE - PRIME 100

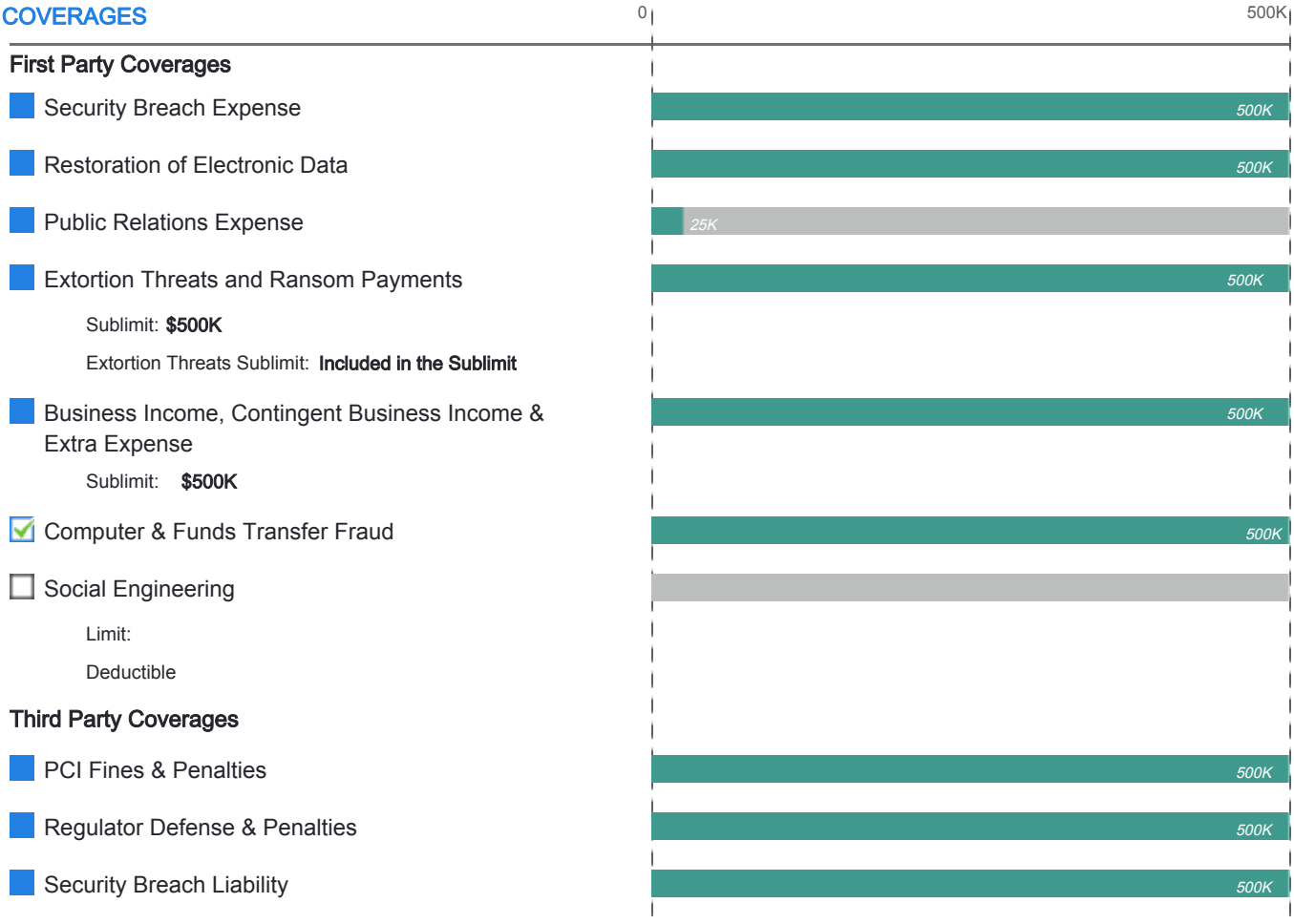
Name of Insured	**Sonora Independent School District**	Agency Name	**HCDT Insurance Agency**
Revenue	**$10,269,946.00**	Insured State	**TX**
# of Employees	**115**	Quote Number	**QCB-100-UNPMBWQQ**
Year Established	**1903**	Expires On	**2024-09-23 (12:01 AM)** Insured Local Time

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.

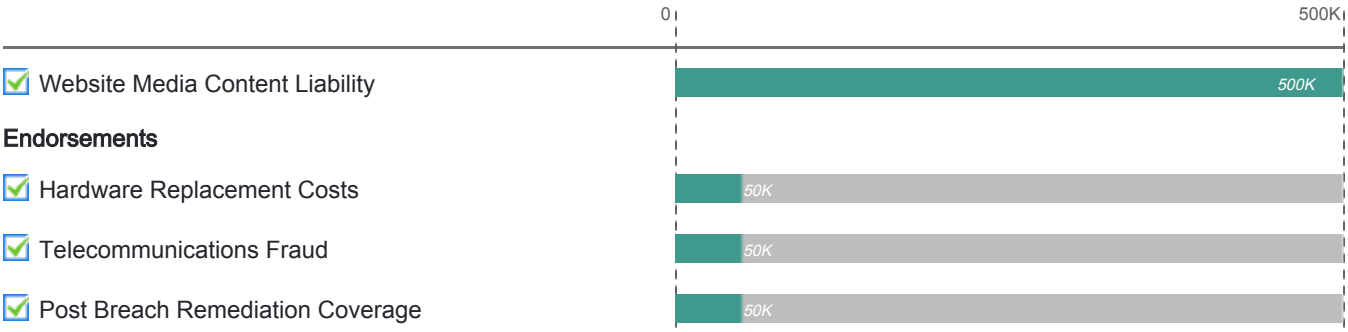
PROPOSED POLICY DETAILS

Aggregate Limit	**$500,000**	Policy Period	**09/01/2024 to 09/01/2025**
Deductible	**$25,000**	Estimated Annual Premium	**$7,811.00**
Waiting Period	**6 Hrs**	Broker Fees	**$25.00**
Retroactive Period	**Full Prior Acts**	Total Amount	**$7,836.00**

COVERAGES



CYBER INSURANCE QUOTE - PRIME 100



LEGEND

Mandatory | Selected | Available | Not Available

DESCRIPTION OF COVERAGES - PRIME 100

(Please note this quote contains only a general description of coverage provided. For a detailed description of the terms, you must refer to the insurance contract itself and the endorsements listed herein).

■ 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.

■ 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.

■ 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.

■ Extortion Threats and Ransom Payments

Coverage for expenses related to the investigation, negotiation, and possible payment of an extortion threat and ransom. This can include fees and costs associated with ransom negotiators, the payment of ransom, interest costs paid to a financial institution for a loan to pay the ransom, and/or reward payments for information leading to an arrest.

■ Business Income, Contingent Business Income & 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 the business interruptions due to system failure or voluntary shutdown are not covered.

☑ Computer and Fund Transfer Fraud

Coverages 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.

☐ Social Engineering

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

■ PCI Fines and Penalties

Coverage for loss and defense expenses as a result of a claim in the form of an action by a Card Company for non-compliance with the Payment Card Industry (PCI) Data Security Standards (DSS), including coverage of related fines or penalties (to the extent such fines or penalties are insured by law).

■ Regulator Defense and Penalties

Coverage for loss and defense expenses as a result of an investigation, demand of Regulatory Proceeding, brought by or on behalf of an administrative or regulatory agency, or any federal state, local or foreign government entity in an official capacity.

☑ Website Media Content Liability

Coverage for 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.

DESCRIPTION OF COVERAGES - PRIME 100

(Please note this quote contains only a general description of coverage provided. For a detailed description of the terms, you must refer to the insurance contract itself and the endorsements listed herein).

■ 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.

☑ 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.

☑ 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.

☑ 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. 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.

LEGEND

■ Mandatory ☑ Selected ☐ Available ☐ Not Available

cowbell®

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

Sonora Independent School District

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 (611110)

Educational Services, Elementary and Secondary Schools

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).