



Cowbell Prime 100

Standalone cyber insurance program for businesses with up to \$100m in revenue.

Risk Appetite:

- Prof. Services
- Insurance Agencies
- Financial Services
- Medical Offices
- Accounting Firms
- Manufacturing
- Dental Offices
- Law Firms
- Retailers
- Hospitality
- Nonprofits
- Contractors
- Truckers
- Wholesale
- Healthcare
- and more!

Admitted in 45 states and D.C. Cowbell delivers standalone cyber insurance nationwide on an admitted, surplus, or excess basis.

Prime 100 delivers essential cyber insurance protection with simplicity and speed:

- Ideal for first-time buyers or businesses upgrading from a BOP or a packaged policy
- Coverages for the diversity of today's cyber threats - not just data breaches
- The ability to customize the policy to the unique risk exposures of every business
- Includes coverage for ransom and extortion, business interruption, social engineering, and fraudulent funds transfer
- Policies written on "A- excellent" rated paper, backed by a panel of top global reinsurers

What's unique about Prime 100

1 Instant bindable quotes

Quote, bind, and issue in less than five minutes.

2 Individualized policies

Coverages that match every business' unique risk profile.

3 Free cybersecurity awareness training

Strengthen the first line of defense for cyber - the employees.

4 [Cowbell Factors™](#)

Continuously updated risk ratings and peer benchmarking.

6 [Cowbell 365](#)

Real-time support from our in-house cyber claims and risk engineering teams.

5 [Cowbell Insights™](#)

Advice to remediate identified exposures and vulnerabilities.

Prime 100 Coverages

The portfolio of coverages in **Cowbell Prime 100** is designed to address the diversity of cyber incidents and resulting damages that can impact businesses.

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.

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.

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.

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.

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 mail by an imposter. A documented verification procedure requirement needs to have been completed in order to be provided coverage.

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.

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 business interruptions due to system failure or voluntary shutdown are not covered.

Website Media Liability

Coverage for the income loss and extra expense due to a system failure (see policy wording) which causes the actual and measurable interruption, suspension, failure, degradation or delay in performance of a service provider's computer system.

Computer & Funds Transfer Fraud

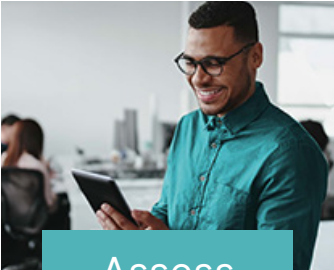


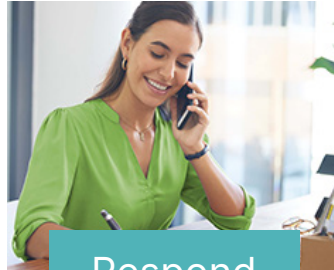
Coverage for the losses due to a fraudulent computer operation that causes money (or other property) to be transferred from an insured's account. This also covers losses incurred by a fraudulent instruction directing a financial institution to debit money from the insured's transfer account.

Value to Policyholders

Closed-Loop Risk Management

Every Cowbell's cyber policy provides value from the day it is issued and throughout the policy period, regardless of whether a cyber event occurs. Our closed-loop approach to risk management -

Assess, Insure, Improve, Respond - enables proactive risk mitigation where cybersecurity and insurance efforts are coordinated.

			
Assess	Insure	Improve	Respond
Use Cowbell Factors™ to quantify your risk exposure and learn exactly how much and what types of coverage your business needs.	With your agent, determine insurable threats and their financial impacts to develop a cyber insurance policy custom-designed to suit your risk profile.	Use our continuous risk assessment and risk insights or ask our Risk Engineering team for guidance to remediate exposure and optimize your premium.	Our cyber claim experts are on-call 24/7 to help you immediately with a full range of post-incident recovery services.

Connect with us! Follow our [blog](#) and [social media](#) to stay up-to-date. Grow your cyber IQ with our insights into cyber insurance, cyber risk, and cybersecurity.

The examples and descriptions provided above are for general, informational purposes only. Notably, these descriptions do not set forth all possible scenarios and/or situations applicable to the described events. Policyholders should be aware that each situation is unique and their experience may not resemble those set forth in the above examples and descriptions. Nor should policyholders in any way rely on the above examples or descriptions as any type of guarantee or indication of how their particular situation will ultimately be resolved. Policyholders should always refer to their own Policy for specific terms and definitions applicable to their Policy. ©2024 Cowbell Cyber, Inc. All Rights Reserved. Cowbell Insurance Agency LLC, State Licenses: <https://cowbell.insure/state-licenses/>