COWBELL™ CYBER

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

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.