

Smart Cyber Insurance from Corvus

Coverage Overview



Corvus's Smart Cyber Insurance™ policies offer broad first-party and third-party coverages, as well as options for additional coverage enhancements. Each policy comes with our Dynamic Loss Prevention Report that provides detailed analysis of your client's cyber security profile and risk-prioritized recommendations for addressing IT vulnerabilities.

THIRD-PARTY COVERAGES

Network Security and Privacy Claims: Claims against you because of a network security or privacy breach. This may arise from a denial of service attack, malicious code, a stolen laptop, or any type of data breach.

Regulatory Investigations, Fines and Penalties: Civil fines and penalties imposed by a governmental agency as a result of a breach of privacy regulations.

Media Liability Claims: Claims against you arising from the release or display of your media material. This includes claims alleging copyright infringement, slander, libel, defamation, and other media perils.

PCI DSS Assessment Expenses: Forensic investigation costs, fines, penalties and assessments you are legally responsible for as a result of actual or alleged non-compliance with Payment Card Industry Data Security Standards.

Breach Management Expenses: Breach response costs for which you have contractually indemnified a third party for a security or privacy breach.

ADDITIONAL COVERAGE ENHANCEMENTS:

- Bricking Coverage
- Forensic Accounting Coverage
- Criminal Reward Expenses
- Invoice Manipulation
- Bodily Injury
- Preventative Shutdown

FIRST-PARTY COVERAGES

Business Interruption: Business income loss and extra expenses you incur during a computer network outage.

Contingent Business Interruption: Business income loss and extra expenses you incur during a network outage at your outsourced service provider.

Digital Asset Destruction, Data Retrieval and System Restoration: Digital asset loss and related expenses you incur as a result of a security breach, privacy breach, or administrative error.

System Failure Coverage: Business income loss, extra expenses, and digital asset loss you incur during an unintentional or unplanned outage.

Social Engineering & Cyber Crime Coverage: Financial fraud, phishing attack loss, and telecommunications fraud loss you sustain as a result of a social engineering event or impersonation attempt.

Reputational Loss Coverage: Business income loss you may suffer related to a media report arising from a privacy breach, cyber extortion threat, or phishing attack.

Cyber Extortion and Ransomware Coverage: Your expenses or payments to respond to a cyber extortion demand or ransomware attack.

Breach Response and Remediation Expenses: Your expenses to respond to a data breach incident including legal services, forensics investigation, notification, credit monitoring and public relations.

Court Attendance Costs: Expenses you incur to attend court, adjudication, mediation or other hearing in connection with a covered claim.