

ABA Cyber for Law Firms

CHUBB®



Are you protected from law firm-related data security exposures?

Depending on the sensitivity of your clientele's non-public information, the level of controversy surrounding cases being handled, or the number of people from whom your law firm collects personally identifiable information, exposure to a data security breach could be worse than you imagine.

Additionally, certain types of work—class actions, workers' compensation cases, personal injury lawsuits, intellectual property, securities and mergers and acquisitions—can leave your firm especially vulnerable to a breach.

Your lawyers professional liability (LPL) policy may protect you from third-party lawsuits, but other, potentially significant expenses may not be covered, such as privacy notification expenses, crisis management expenses, business interruption, extortion threats, the recovery of vandalized data, and regulatory fines and penalties.

A distinctive level of cyber protection that only Chubb can offer

Chubb has handled cyber incidents and underwritten cyber exposures for policyholders for more than 15 years.

Over this time, Chubb has cataloged and analyzed a considerable amount of loss data, resulting in our three-prong approach to cyber underwriting that incorporates risk transfer, loss mitigation services and post-incident services.

Why? Because technology and cyber risks are enterprise-wide issues that require an enterprise-wide solution: Chubb's Cyber Enterprise Risk Management Policy (Cyber ERM).

With Cyber ERM, you can have access to coverage that builds on all of the Chubb cyber products that have come before it, incorporating insight gained from years of claims and underwriting experience. This premier coverage is backed by the financial strength of Chubb's A++ balance sheet¹ and supported by Chubb's extensive cyber services:

- Loss Mitigation Services - access to the tools and resources needed to address and gauge key areas of cyber security risks before an event occurs.
- Incident Response Services - a diverse team of experts in the legal, computer forensics, notification, call center, public relations, fraud consultation, credit monitoring, and identity restoration service to help limit exposure to a loss when an event occurs.

Key Features

- Industry-leading coverage designed to address evolving regulatory, legal and cybersecurity standards and built to consider future changes
- Easy-to-read form:
 - Structure aligned with the flow of a typical incident
 - Presentation of Cyber Incident Response Expenses aligned with the typical flow of decision-making throughout an incident
- Clearly labeled exclusions with competitive carve-backs
- Payment Card Loss coverage built into the base form
- Discovery-based coverage at a Control Group level
- Includes enhanced Business Interruption and Extra Expense language
- Broadened definition of Protected Information includes biometrics, internet browsing history and personally identifiable photos and videos
- Extortion Expenses explicitly include Bitcoin and other cryptocurrencies
- Coverage Territory applicable to anywhere in the universe to address continued evolution of hosting and data storageⁱⁱ

Coverage Synopsis

The following coverages are available with Cyber ERM:

Third-Party Liability Coverage

- Cyber, Privacy and Network Security Liability: Failure to protect private or confidential Protected Information of others, and failure to prevent a Cyber Incident from impacting the systems of certain other parties
- Payment Card Loss: Most contractual liabilities owed as a result of a Cyber Incident
- Regulatory Proceedings: Defense for regulatory actions
- Electronic, Social and Printed Media Liability: Copyright and trademark infringement within scope of defined media content

First-Party Coverage

- Cyber Incident Response Fund: Legal fees, forensics, notification costs, credit monitoring, public relations, etc.
- Business Interruption: Loss of profits and expenses from interruptions of insured's systems; and with Contingent Business Interruption, adds losses from interruptions of the systems of certain other parties
- Digital Data Recovery: Costs to restore or replace lost or damaged data or software
- Telephone Toll Fraud: Costs incurred as phone bill charges due to fraudulent calling
- Network Extortion: Payments to prevent digital destruction/impairment

The Chubb difference

- For more than 30 years, we've devoted ourselves to helping to protect law firms like yours. Today, 95% of the top 200 U.S. law firms are insured with Chubb.
- Leading provider of cyber risk solutions since first product was launched in 1998
- Extensive claims experience - helped notify more than 300 million individuals of a privacy breach

Contact Us

To learn more about Cyber ERM for law firms, visit ABAinsurance.com.

ⁱ "A++ balance sheet" refers to the rating by A.M. Best as of February 2017 for the majority of the Chubb companies.

ⁱⁱ Any provision in the Policy pertaining to coverage for Incidents, Claims made or Damages or Claims Expenses sustained anywhere outside the United States of America shall only apply where legally permissible.

Chubb. Insured.SM

The American Bar Association (ABA) has selected Chubb as the preferred provider of cyber liability insurance for its members.

Chubb is the marketing name used to refer to subsidiaries of Chubb Limited providing insurance and related services. For a list of these subsidiaries, please visit our website at www.chubb.com. Product highlights are summaries only. Please see the actual policy for terms and conditions. Products may not be available in all locations, and remain subject to Chubb's underwriting criteria. Surplus lines insurance is sold only through licensed surplus lines producers.

Form 72-01-0040 (Ed. 6/17)