Coalition

THE CYBER SAVVY BROKER'S GUIDE

Cyber Insurance for the Legal Industry

Maintaining trust and security is a major concern for most professional service organizations and is especially true for those in the legal industry. Many legal organizations prioritize data privacy and cybersecurity to help avoid costly breaches and incidents that could damage their reputation or way of doing business.

Legal organizations operate based on competency, trust, and confidentiality. As part of the duty of competent representation, lawyers are ethically bound to become and remain technologically competent, which includes keeping up with changes in technology or data protection laws that may affect their practices. Legal organizations are also bound to protect client privilege and confidentiality. A breach or security incident that is handled improperly can have major implications that go beyond direct expenses and cross into cyber liability and in some cases professional liability territory.

Claims Insights

It's just a little security incident. How bad could it be?

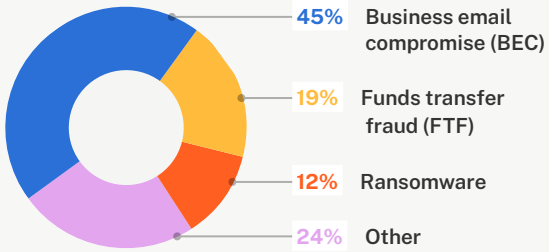
$104,000

Average net loss in a cyber insurance claim for legal organizations

Claim Examples

ORGANIZATION	EVENT TYPE	LOSS
Family Law	Business Email Compromise	$106,000
General Practice	Funds Transfer Fraud	$68,000
Probate	Ransomware	$481,000

Cyber Claims by Event Type



Source: Coalition claims data

KEY INSIGHT —— Although it's not the leading event type, the average ransomware loss for organizations in the legal industry is more than $310,000.

Coalition, Inc. · 55 2nd Street, Suite 2500, San Francisco, CA 94105 · coalitioninc.com

Coalition

Unique Exposures

Most legal organizations use data and technology. Why is that risky?

Essential Technologies Can Create Cyber Risk

Client portals

These platforms enable lawyers to securely share documents, messages, and invoices with clients. Unauthorized access of a client portal could compromise sensitive information and lead to additional cyber events.

Customer relationship management (CRM) systems

CRM systems are used to support business development activities. Containing client data and confidential corporate information, CRM systems could be compromised and leveraged for malicious purposes, resulting in a data breach.

Document management systems

These software platforms are used to store and handle a large volume of shared files. However, a compromise could expose sensitive data and cause serious disruptions due to the volume and potentially sensitive nature of the information in these systems.

eDiscovery tools

These tools can save time and effort when reviewing large volumes of information, but the potentially sensitive nature of the data means unauthorized access could have data privacy and business interruption implications.

Email

Business email compromise (BEC) is a frequent cause of cyber insurance claims for legal organizations, which can trigger data breaches, business interruption and even reputational damage.

Payment processing software

Funds transfer fraud (FTF) and invoice manipulation are major drivers of cyber insurance claims. For law firms that use electronic payments, even one fraudulent transfer can have dire financial consequences.

Law practice management software

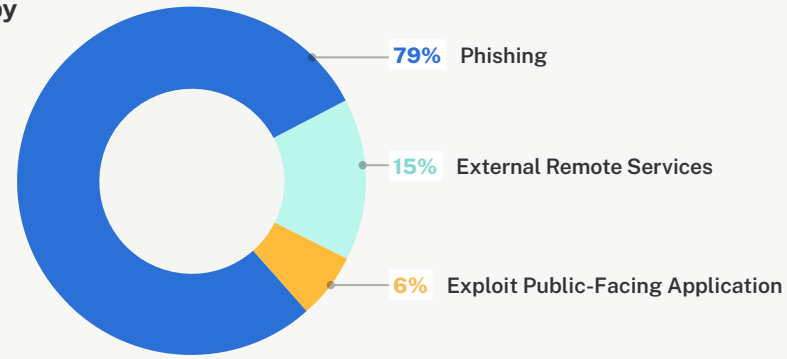
These systems are used to manage operations, such as scheduling, billing, and payments. A breach could cause serious disruption and expose payment information, corporate confidential data, and client data.

Social media

Many law firms use social media to interact with clients and share information, but compromise or misuse of these platforms by employees or attackers could have serious implications on its reputation and public image.

Cyber Claims in the Legal Industry by Attack Vector

KEY INSIGHT —— Phishing isn't associated with one event type; it's simply how attackers get into a system. Once inside, they can pursue all sorts of malicious activities, which is why **phishing is the leading attack vector for all cyber claims**.



Source: Coalition forensics survey data

Coalition

Sensitive Data Can Increase Business Liability

Corporate confidential data
Corporate law firms may have access to internal operations data, intellectual property, or trade secrets. Mishandling or leaking corporate confidential data can cause significant damage to the data owner.

Financial data
Collecting and processing financial information requires adherence to industry standards. Mishandling or unauthorized disclosure of financial data can cause direct harm to clients and even trigger industry and regulatory investigations.

Personally identifiable information (PII)
PII is any data that can potentially identify a specific person. PII can be used to launch cyber attacks or gain access to networks to initiate attacks. Organizations that mishandle PII or fail to respond to a data breach appropriately can be subject to fines, penalties, and other financial damages.

Non-sensitive personal information
Some data may be publicly available and not considered protected, but a breach can still impact trust and public image if it appears the organization did not handle the situation appropriately.

Protected health information (PHI)
Many law firms collect or access PHI, and some operate as HIPAA business associates, which means they carry additional data protection and reporting requirements if an actual or suspected data breach occurs.

Sensitive employee information
Every organization collects and stores information about its employees. Unauthorized access or disclosure of this data — whether PII, PHI, financial, or otherwise — can cause direct harm to employees.

Examples of Legal & Regulatory Compliance

- Data privacy & security contractual obligations
- Health Insurance Portability & Accountability Act (HIPAA)
- International data privacy and consumer protection regulations (e.g. GDPR)
- Payment Card Industry Data Security Standard (PCI DSS)
- State data privacy & consumer protection laws (e.g. CCPA)
- State notification requirements

$4.7 million

Average total cost of a **data breach** for legal organizations[1]

1. IBM Security, Cost of a Data Breach Report 2022

Coalition, Inc. · 55 2nd Street, Suite 2500, San Francisco, CA 94105 · coalitioninc.com

Coalition

Business Impacts

What can legal organizations expect after a cyber incident?

Direct costs to respond

Responding to a cyber event typically requires numerous direct costs, also known as first-party expenses. If a legal organization experiences BEC and sensitive data is involved, it can trigger a need for additional legal counsel, forensic investigation, victim remediation, and notification. Simple investigations can cost tens of thousands of dollars, while more complex matters can increase costs exponentially. Relevant insuring agreements may include:

- Bodily Injury and Property Damage - 1st Party
- Breach Response
- Crisis Management
- Cyber Extortion

Liability to others

The evolving data privacy landscape can be difficult to navigate, and many law firms can face new and unexpected exposures after a cyber event. Even with strong contracts, policies, and best practices in place, a data breach or security failure can trigger liability to third parties and expose an organization to regulatory investigations and legal action from victims. Relevant insuring agreements may include:

- Bodily Injury and Property Damage - 3rd Party
- Multimedia Content Liability
- Network and Information Security Liability
- PCI Fines and Assessments
- Pollution
- Regulatory Defense and Penalties

Business interruption and reputation damage

A cyber event that impacts essential technology can have a significant impact on a legal organization's ability to operate and can be highly visible to clients, customers, and other stakeholders. Every hour of disruption can lead to direct loss of revenue and inhibit a law firm's ability to support clients, negatively impacting client retention and acquisition. Relevant insuring agreements may include:

- Business Interruption & Extra Expenses
- Reputation Repair

Cybercrime

Beyond ransomware and data breaches, cyber events can result in financial theft for a law firm or its clients — often without an actual breach. If an attacker dupes someone in the billing department to alter payment instructions, a legal organization can lose tens or hundreds of thousands of dollars almost instantly. Attackers can also gain access to email accounts and send fraudulent invoices or payment instructions to clients, customers, and other third parties. Relevant insuring agreements may include:

- Funds Transfer Fraud
- Invoice Manipulation
- Phishing (Impersonation) and Proof of Loss Preparation Expense Endorsement
- Service Fraud

Recovery and restoration

After a cyber event, resuming operation is no easy task. If an attacker damages or destroys essential technology, data, or physical equipment, a legal organization may need to bring in external support or purchase new equipment to re-secure systems. Full remediation, restoration, and recovery can take a significant amount of time, when possible, and may require purchasing new software, systems, and consultants to rebuild the network. Relevant insuring agreements may include:

- Computer Replacement
- Digital Asset Restoration

Coalition

Cyber Insurance Reimagined

How does Coalition perform?

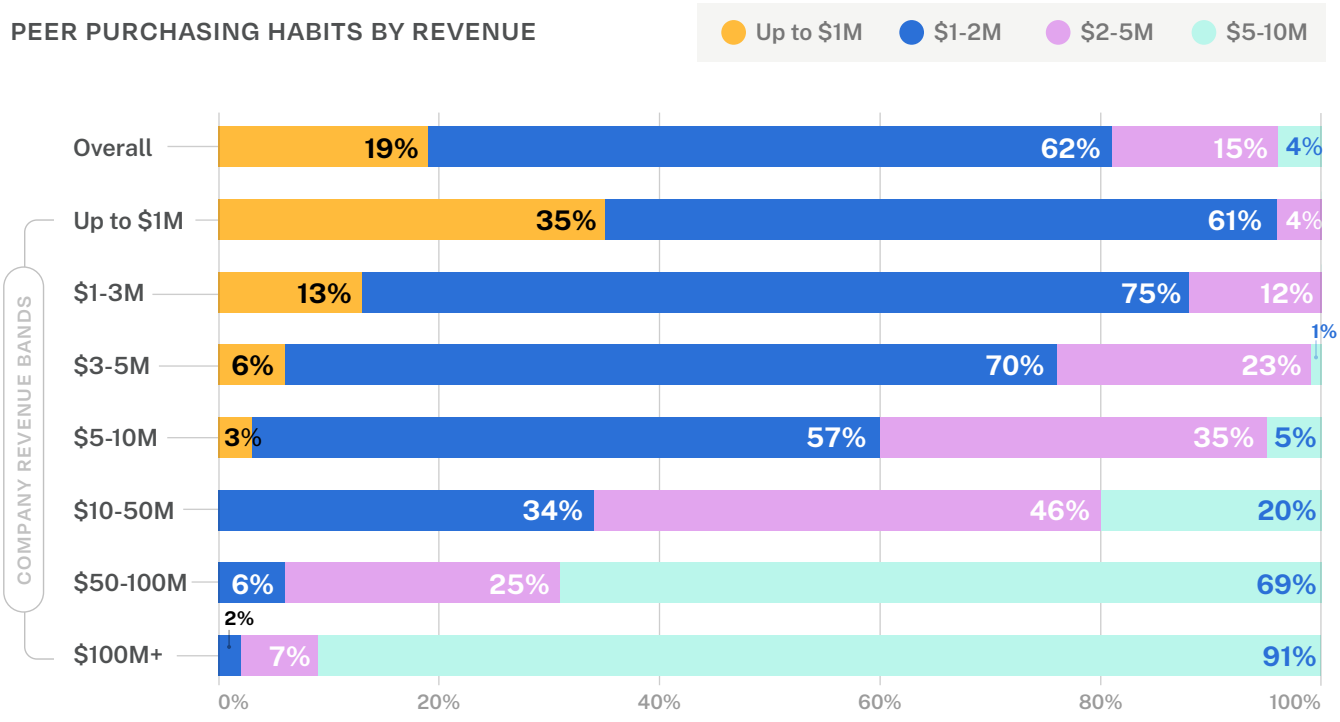
1.87%
Coalition 2022 overall claims frequency

↓ 22%
Year-over-year decrease in Coalition claims frequency

64% fewer
Coalition claims vs. cyber industry average

Peer Purchasing Insights

Primary limit amounts purchased by others in the legal industry



Source: Coalition policyholder data

KEY INSIGHT —— Most small and medium-sized businesses in the legal industry purchase $1M-2M in limits, while many mid-market businesses purchase $5-10M in limits.

Coalition, Inc. · **55 2nd Street, Suite 2500, San Francisco, CA 94105** · **coalitioninc.com**

Coalition

The Power of Active Insurance

Why do legal organizations choose Coalition?

47%	43%	73%
Reported cyber events handled with no cost to policyholder	Reduction in critical vulnerabilities among policyholders in 2022	Average decrease in ransomware payment amount via negotiation

Active Insurance* is designed to help prevent digital risk before it strikes. Our new approach to managing digital risk provides **three layers of support**:

Active Protection

Monitoring and alerting to identify and prevent risk before it strikes

Active Risk Assessment

Underwriting, quoting, renewals, and digital risk scores powered by real-time data

Active Response

Access to in-house resources that accelerate response and coverage if an incident occurs

Insurance as active as digital risk

In the digital economy, Coalition wants to ensure that all organizations can thrive by helping to protect them from the threat of emerging risks. We've built an expert team across incident response, claims, and our panel vendors. In the event of a claim, Coalition helps organizations respond and recover so they can get back to business.

Brokers

Get appointed today at signup.coalitioninc.com

Legal organizations

Get a free risk assessment at control.coalitioninc.com

Coalition, Inc. · 55 2nd Street, Suite 2500, San Francisco, CA 94105 · coalitioninc.com