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 organisations and is especially true for those in the legal industry. Many legal organisations prioritise data privacy and cybersecurity to help avoid costly breaches and incidents that could damage their reputation or way of doing business.

Legal organisations 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 organisations 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?

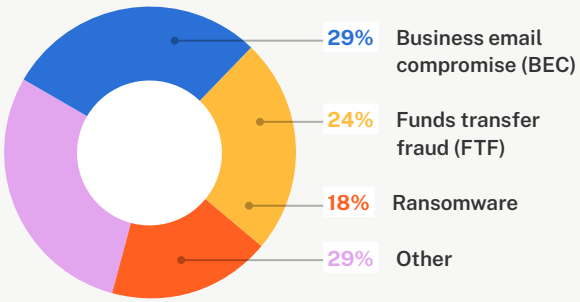
$113,000

Average net loss in a cyber insurance claim for legal organisations

Claim Examples

ORGANISATION	EVENT TYPE	LOSS
Family Law	Business Email Compromise	$159,000
General Practice	Funds Transfer Fraud	$102,000
Probate	Ransomware	$722,000

Cyber Claims by Event Type



Source: 2023 Coalition claims data

KEY INSIGHT —— Although it's not the leading event type, the average ransomware loss for organisations in the legal industry is more than $183,000.

Unique Exposures

Essential Technologies Can Create Cyber Risk

Client portals
These platforms enable lawyers to securely share documents, messages, and invoices with clients. Unauthorised 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 unauthorised access could have data privacy and business interruption implications.

Email
Business email compromise (BEC) is a frequent cause of cyber insurance claims for legal organisations, 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.

CASE STUDY

Law Firm Chooses to Pay Ransom and Protect Client Data Due to Exfiltration

After experiencing a ransomware attack, a law firm took measures into its own hands and attempted to restore its systems from backups. Working with a managed service provider (MSP), the firm thought things were under control until it learned the threat actor had exfiltrated its data and threatened to leak it. That's when the company contacted Coalition.

Initially, the law firm was hesitant to investigate the matter but suddenly felt an urgency to pay the ransom and protect their client data. The firm selected Coalition Incident Response[1] (CIR) to begin the forensics investigation. The threat actor claimed to have stolen more than 100 GB of data, but CIR suspected it could be much more.

To determine what data was exfiltrated and which individuals would need to be notified, CIR engaged the threat actor and requested evidence of the stolen data. Ultimately, CIR negotiated the six-figure ransom down to less than half of the initial demand. The threat actor also provided video confirmation of the files being deleted.

CIR concluded that no additional data had been compromised beyond the amount the threat actor initially claimed was stolen. Here's how the law firm's policy responded: Cyber Extortion covered the entire ransom payment. Breach Response covered the costs of breach counsel and CIR investigation. After the law firm paid its $5,000 self-insured retention, its policy covered more than $250,000 in costs related to this claim.

1. Coalition Incident Response services provided through Coalition's affiliate are offered to policyholders as an option via our incident response firm panel.

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 unauthorised 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. Organisations 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 organisation did not handle the situation appropriately.

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

Sensitive employee information
Every organisation collects and stores information about its employees. Unauthorised 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
- Privacy Act of 1988
- International data privacy and consumer protection regulations (e.g. GDPR)
- Payment Card Industry Data Security Standard (PCI DSS)
- State notification requirements

$4.47 million

Average total cost of a **data breach** for legal organisations[3]

3. IBM Security, Cost of a Data Breach Report 2022. Dollar figures adjusted to Australian Dollars.

Business Impacts

What can legal organisations 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 organisation 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 organisation 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 Defence and Penalties

Business interruption and reputation damage

A cyber event that impacts essential technology can have a significant impact on a legal organisation'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 organisation 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 organisation 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

Cyber Insurance Reimagined

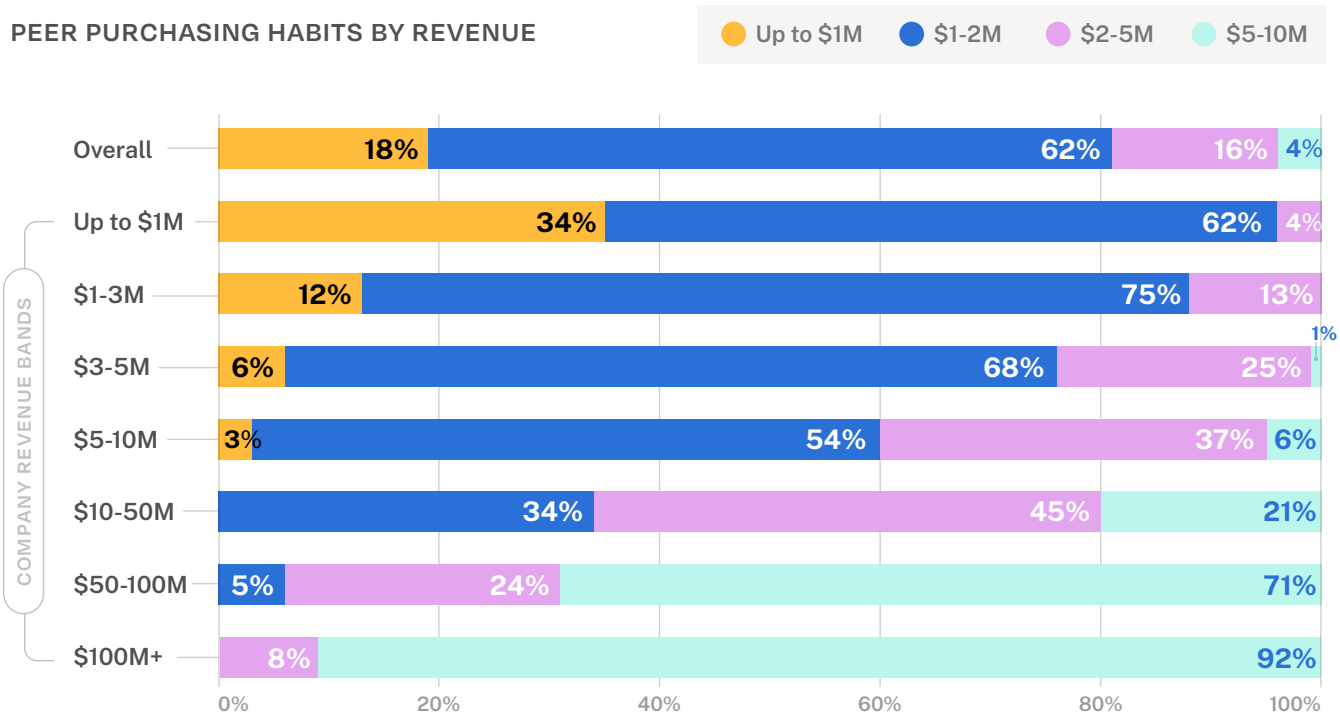
How does Coalition perform?

64%	$38 million	$470,000
Average ransom reduction from initial demand via negotiation	Total amount recovered by Coalition from FTF in 2023	Average recovery amount per FTF claim when successful

Source: Coalition, 2024 Cyber Claims Report

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 offers primary terms for businesses up to $2B in turnover.

The Power of Active Insurance

Why do technology businesses choose Coalition?

64% fewer
Coalition claims vs. cyber insurance industry average

52%
Reported matters handled with no out-of-pocket payments

5 minutes
Average response time to a cyber incident

Cyber risk evolves quickly, with new threats constantly emerging. Traditional insurance providers lack the visibility and tools to keep up with these new, fast-paced digital risks.

ASSESS
Real-time, external view of cyber risk with customized recommendations

PROTECT
Identify and prevent new threats with tailored remediation guidance and support

COVER
Comprehensive coverage to give peace of mind following an attack

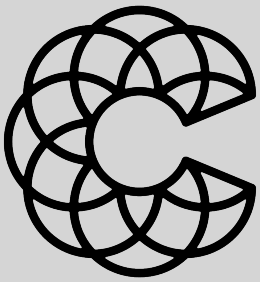
RESPOND
Immediate expert support to minimize impact and speed up recovery

The Coalition Advantage

Hundreds of thousands of businesses protect their businesses with Active Insurance. While other cyber insurance providers wait for a claim to engage, we use data and security insights to partner with you and help mitigate digital risks throughout the life of your policy. Comprehensive cyber coverage, innovative security tools, and world-class claims handling allows Coalition policyholders to focus on growing their business with protection and greater peace of mind.

Brokers
Get appointed today at signup.coalitioninc.com

Technology businesses
Get a free risk assessment at control.coalitioninc.com



Coalition®

COALITIONINC.COM

COALITION INSURANCE SOLUTIONS, INC.

44 MONTGOMERY STREET, SUITE 4210, SAN FRANCISCO, CA 94104

HELP@COALITIONINC.COM