

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?*

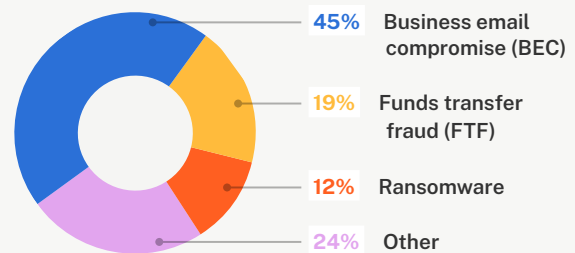
£86,300¹

Average net loss in a cyber insurance claim for legal organisations

Claim Examples²

ORGANISATION	EVENT TYPE	LOSS
Mid-size Law Firm	Business Email Compromise	£80,000
Barrister's Chambers	Business Email Compromise	£35,000
Conveyancer	Funds Transfer Fraud	£50,000

Cyber Claims by Event Type¹



Source: Coalition Inc. claims data 2023

KEY INSIGHT — Although it's not the leading event type, the average ransomware loss for organisations in the legal industry is more than £138,400¹.

¹ Coalition's 2023 Cyber Claims Report. Dollar figures adjusted to British Pounds.

² Statistics sourced from Coalition's UK claims data.

Unique Exposures

Most legal organisations 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. 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 organisations², 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 claims², as many legal firms send invoices by email. But even one fraudulent transfer can have dire financial consequences.

Legal practice management software

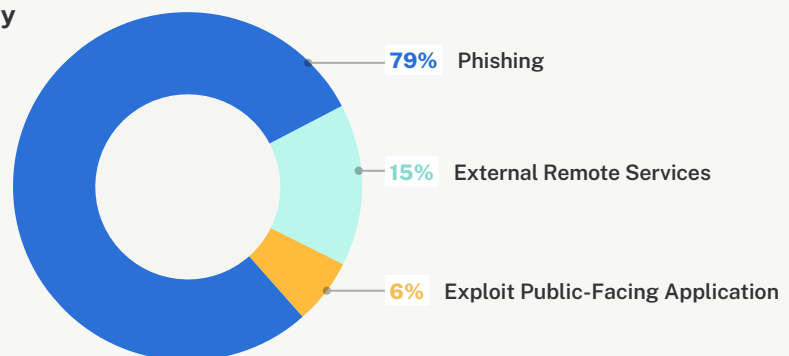
These systems are used to manage operations, such as scheduling, billing, and payments. A breach could cause serious disruption and expose payment information, corporate confidential data, and client data.

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 Vector¹

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**.



¹ Source: Coalition Incident Response (CIR) forensics global survey data. CIR is an affiliate of Coalition Risk Solutions Limited.

² Source: Global data from 2024 Coalition Inc. Cyber Claims Report

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
- UK & International data privacy and consumer protection regulations (e.g. GDPR)
- Data privacy and consumer protection laws
- Payment Card Industry Data Security Standard (PCI DSS)
- Compliance with standards of legal regulatory bodies

£3.4 million

Average total cost of a **data breach** for legal organisations globally³

3. IBM Security, *Cost of a Data Breach Report 2022*. Dollar figures adjusted to British Pounds.

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 pounds, 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 Assessments¹
- Pollution
- Regulatory Defence and Penalties¹

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 pounds 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 operations can be 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

¹. Offered coverages to the extent insurable under applicable law. Exclusions and limitations apply.

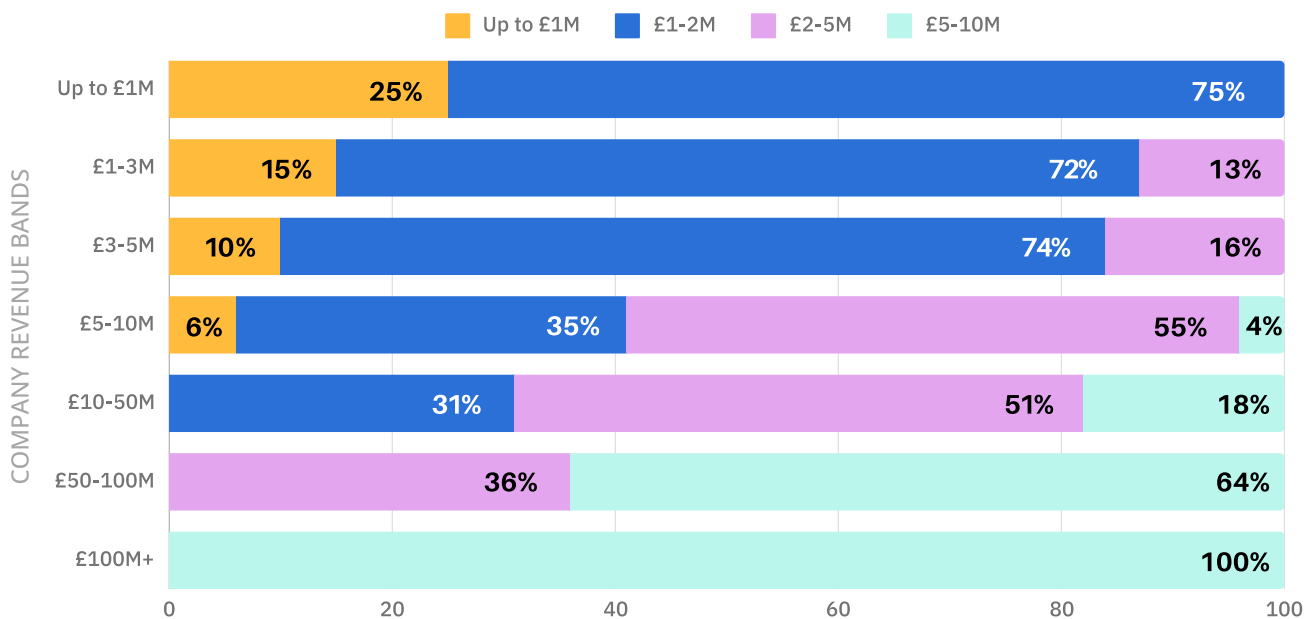
Cyber Insurance Reimagined

How does Coalition perform?



Peer Purchasing Insights

Primary limit amounts purchased by others in the legal industry



Source: Coalition UK 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 £1B in turnover.

1. Global data from Coalition Inc. 2024 Claims Report

The Power of Active Insurance

Why do legal organisations choose Coalition?



The Coalition Advantage

Globally, hundreds of thousands of policyholders help protect their organisations from digital risk with Active Insurance. While traditional cyber insurers wait for a claim to engage, Coalition² use data and security insights to partner with brokers and insureds to help mitigate digital risks throughout the life of a policy. Comprehensive cyber coverage, innovative security tools², and responsive claims handling allows policyholders to focus on everyday operations with greater peace of mind.

Brokers

Get appointed today at coalitioninc.com

Legal organisations

Get a free risk assessment at trycontrol.coalitioninc.com

1. Global data from Coalition Inc. 2024 Claims Report

2. Security tools, data and services provided by Coalition Inc.