RYAN SPECIALTY

FINANCIAL LINES CYBER

Law Firms

Innovative Insurance Solutions for Complex Cyber Risks

RYAN SPECIALTY | FINANCIAL LINES CYBER

Cyber Exposure for Law Firms

For today's law firms, cybersecurity risk has become inseparable from day-to-day operations. With vast stores of sensitive client information, high-value wire movements, and increased reliance on cloud-based tools, the legal sector presents a uniquely attractive target for cybercriminals. Breach frequency and severity continue to rise, and even short disruptions can have a lasting impact.

Reliance on Technology

In an effort to manage margins and enhance data accessibility, many law firms have invested heavily in technology designed to support a range of administrative and operational functions. From the routine task of logging billable hours to hosting virtual data rooms, automated processes and access to these services are critical. Technological evolution has affected how law firms function and ultimately earn revenue.

Dependence on technology increases the potential for a business interruption event, and the centralisation of data repositories heightens the risk of large-scale breaches. These disruptions can carry real operational and financial consequences for law firms as the sector increasingly adopts technology to enhance efficiency, accuracy, and client service.

Key technologies include:

- **Legal Research Tools**: Advanced databases and AI-powered tools assist lawyers in conducting thorough legal research.
- **Case Management Systems**: These systems streamline the management of cases, documents, and client information.
- **E-Discovery**: Technology aids in the identification, collection, and analysis of electronic data for legal proceedings.
- **Virtual Law Firms**: Remote working tools and cloud-based platforms enable lawyers to work from anywhere, enhancing flexibility and client access.

Cybersecurity Threats

Law firms are a keen target for criminal actors due to their role in managing sensitive data, as well as large ticket wire transfers on behalf of clients. In 2024, the number of successful cyber attacks against UK law firms increased by 77%,[1] and a study by Cert-UK revealed that 65% of law firms have been victims of cyber incidents.[2] Similarly, a 2025 survey found that 20% of law firm respondents experienced a cyber attack within the previous 12 months.[3]

Moreover, it is not only large law firms that are at risk. Small and midsize firms hold valuable information that attracts cybercriminals and may collect data on a volume their infrastructure cannot securely support. For example, a firm representing multiple clients in a case against a hospital may maintain extensive medical records. The regulatory fines associated with a breach of Protected Health Information (PHI) / Special Category Data can be significant, and some smaller law firms may not realize, that by collecting this data, they have effectively become aggregators of Personally Identifiable Information (PII) or PHI / Special Category Data, creating a substantial exposure.

1 White, S. (2025). The Law Society. The Law Society. https://www.lawsociety.org.uk/topics/business-management/partner-content/five-challenges-for-the-legal-sector-in-2025

2 Doswell, J. (2024, March 20). As cybercriminals use AI to escalate threats, how can law firms protect themselves? www.lawsociety.org.uk. https://www.lawsociety.org.uk/topics/cybersecurity/partner-content/as-cybercriminals-use-ai-to-escalate-threats-how-can-law-firms-protect-themselves

3 How law firms can prevent cyberattacks | Proton | Proton. (2025, July). Proton. https://proton.me/blog/law-firms-cyberattacks

Regulatory Exposure

Law firms must comply with a range of regulations designed to protect sensitive information and uphold cybersecurity standards including, as examples*:

- **General Data Protection Regulation (GDPR)**: In Europe, GDPR mandates the protection of personal data and imposes strict penalties for non-compliance. This is mirrored in UK law under the Data Protection Act 2018.
- **American Bar Association (ABA) Model Rules of Professional Conduct**: In the US, these rules obligate lawyers to take reasonable steps to protect client information, including maintaining appropriate data security measures.
- **Cybersecurity and Infrastructure Security Agency (CISA)**: In the US, CISA provides guidance, best practices, and resources to help organisations, including law firms, protect critical infrastructure and strengthen their cybersecurity posture.
- **Solicitors Regulation Authority (SRA)**: In England and Wales, the SRA may investigate firms following cybersecurity incidents. When a firm is found to have inadequately managed its cyber risks, the SRA may impose fines or other sanctions.

*Representative examples only; not a complete list.

The Impact of Cyber Attacks

Cyber attacks on law firms can have severe consequences:

- **Operational Disruptions**: Attacks can lead to delays in legal proceedings, missed deadlines, interruptions to critical workflows, and broader operational inefficiencies.
- **Financial Losses**: Law firms can incur significant costs due to system downtime, data recovery, and regulatory fines.
- **Compromised Client Relationships**: Cyber incidents may result in a collapse in client confidence, lead to the loss of key relationships, and in some cases trigger class action allegations or other resultant legal disputes.
- **Reputational Damage**: A breach could potentially result in a firm being excluded from tender processes requiring cybersecurity certifications, challenges in attracting top talent concerned about operational stability, or a decline in referral rates from other professional services firms.
- **Increased Professional Indemnity Insurance Premiums**: A cyber incident, especially one involving data breach or ransomware, may signal an elevated risk profile to insurers. A history of claims can lead to higher premiums or limitations in coverage at renewal, particularly for firms relying on endorsements or “silent” cyber protections within their Professional Indemnity policies.

Illustrative Loss Scenarios

BUSINESS INTERRUPTION

A prominent law firm experiences a ransomware attack that encrypts its case management and document storage systems. As a result, the firm is unable to access critical case files, leading to delays in court proceedings and client consultations.

The financial impact is substantial, with the firm losing an average of $500,000 per day due to the downtime, which lasts for three days. This results in a total financial loss of $1.5 million. Additionally, the firm incurs costs related to data recovery, system upgrades, and enhanced cybersecurity measures to prevent future attacks.

PRIVACY BREACH

A large law firm suffers a significant privacy breach when cybercriminals gain unauthorized access to its client database, compromising sensitive personal and financial information of over 50,000 clients.

The financial impact is severe, with the firm facing immediate costs for notifying affected clients, providing credit monitoring services, and conducting a thorough investigation, totaling $2 million. Additionally, the firm incurs legal fees and regulatory fines amounting to $3 million. The breach also damages the firm's reputation, leading to a decline in client trust and an estimated revenue loss of $1 million over the next year.

THIRD PARTY

A major law firm experiences a third-party compromise when a vendor responsible for managing its billing systems is breached. The cyber attack disrupts the billing operations, exposing sensitive client financial information. The breach affects over 30,000 clients, including personal and financial information.

The financial impact is significant, with the firm incurring immediate costs for notifying affected clients and providing credit monitoring services, totaling $1 million. Additionally, the firm faces legal fees and regulatory fines amounting to $2 million. The breach also leads to a loss of client trust, resulting in a decline in new client registrations and an estimated revenue loss of $800,000 over the next year.

These examples are hypothetical scenarios used solely to illustrate potential outcomes and not reflective of policy terms and conditions or the facts of a specific claim.

RFL's Cyber Solution

Ryan Financial Lines' (RFL) policy was created to look at cyber as a peril, considering how data and systems can cause a wide array of operational challenges. Addressing areas such as business interruption, data restoration, computer crime and social engineering, extortion, and privacy breaches, RFL's tailored policy is here to help in a time of crisis, offering a blend of 1st party cost reimbursement and 3rd party defence and regulatory coverage, aided by our broad definition of data and computer systems.

1ST PARTY

Crisis Response: Intended to help mitigate the costs and expenses to respond to a system event or privacy breach event

Cyber Extortion: Intended to help mitigate the costs and expenses to respond and resolve an extortion demand that threatens to release or destroy data and/or disrupt or damage the computer system

Computer System Interruption: Intended to help mitigate the net income losses and additional operating costs that occur during a business interruption event due to systems and/or data being taken offline in a malicious attack or other operational failure

Coverage can include:

- Renting, leasing, or hiring external equipment to reduce the duration of a material interruption
- Additional operating costs including services, premises, employing contract staff, and overtime cost
- Costs to switch service from a named IT vendor to a new provider if the service cannot be restored within the indemnity period (when event is caused by vendor systems)
- Procuring product or services from alternative sources to meet contractual obligations in supplying the insured's customers
- Paying any service credits or contractual penalties that the insured is contractually required to pay as a result of a material interruption

Reputational Damage: Intended to help mitigate the loss of net income due to a reduction in business or the loss of a service contract with a client in the wake of the public being notified of a system event, privacy breach event, or network security event

Fraud and Social Engineering: Intended to help mitigate the direct financial loss from the wrongful transfer of money by fraudulently accessing the computer system or intentionally misleading an authorized person to transfer funds to a third party purporting to be a vendor, client, or employee. This cover also extends to the financial loss arising from the unauthorized access of a client's telecommunication system by a malicious third party

Data and Software Restoration: Intended to help mitigate the costs and expenses to recover corrupt data or software, and potentially even upgrading or replacing affected software applications or equipment

3RD PARTY

Privacy Breach and Other Third-Party Liability:

Intended to help mitigate the defence costs and damages arising from:

- Any unauthorized disclosure or access to personal or confidential corporate data
- Any liability that arises from other cyber events such as the transmission of a malicious code, contract breaches due to a BI event, and unauthorized access to data by a third party

Vendors

In a time of crisis, RFL aims to provide insureds with access to a vendor panel to assist in mitigating the impact and to make the claims process as straightforward as possible. In addition, RFL's cyber solution not only offers breach-response support options but also connects insureds with a panel of reputable vendors who can help reduce the likelihood of a cyber event.

Privacy Counsel: US

Pierson Ferdinand LLP

Incident reporting:

RFLCyber@pierfed.com

833-737-7444

Alternate counsel options:

McDonald Hopkins LLC

Cipriani & Werner, PC

Mullen Coughlin

Wood Smith Henning & Berman LLP

Privacy Counsel: Intl.

Kennedys Law LLP

Incident reporting:

RyanFinLinesIR@kennedyslaw.com

UK/EMEA- +44 203 137 8749

AUS/APAC- +613 9498 6688

Alternate counsel options:

Weightmans LLP

Pinsent Masons LLP

Forensics: US

CyXcel

S-RM

Kroll

IronGate

CrowdStrike

PNG Cyber

Palo Alto Networks - Unit 42

Data Mining

CyXcel

Consilio

Asceris

Epiq

Notifications

IDX

Epiq

Kroll

Forensics: Intl.

CyXcel

S-RM

Please note that the use of these vendors is subject to the terms, conditions, and reporting requirements outlined in your policy. We reserve the right to amend our vendor panel at any time.

RYAN SPECIALTY | FINANCIAL LINES CYBER

Who We Are

Ryan Financial Lines was formed in March 2024 to offer clients a wide-ranging, single platform of financial lines products. Ryan Financial Lines brings together the Management and Professional Liability talent at Ryan Specialty Underwriting Managers providing greater synergies and efficiencies to further enhance the solutions and services for our clients and carriers. This unified approach brings together our expanding network of expertise of more than 70 teammates based across a number of key territories, including North America, United Kingdom, Europe and Latin America.

ryanfinlines.com

International: RFL-UK-Cyber@ryanfinlines.com | US: RFL-US-Cyber@ryanfinlines.com