Gallagher

Insurance | Risk Management | Consulting

Law firms are increasingly attractive targets for cybercriminals — but what can you do about it?

Cybercriminals typically have three objectives when they attack a business: money, status, and data. The ecosystem for cybercrime has evolved rapidly in recent years, with the latter becoming increasingly important. As law firms hold a wealth of privileged information, hackers now see them as lucrative watering holes for data.

Recent figures from insurer Chaucer attest to this growing awareness: the number of reported cyber breaches at UK law firms increased by 36% in 2022/23. The Information Commissioner's Office (ICO) reported 226 breaches in the year up to 30 September 2023, compared to 166 in the previous year.[1]

Despite this increase in cyber vulnerability, according to our industry research, only around 20% of lawyers currently purchase cyber cover. Compared to other industries, law firms may also have limited cybersecurity measures in place, increasing their vulnerability to cyberattacks, as hackers often exploit weaknesses in security systems, outdated software, or inadequate employee training.

The nature of the beast

By their nature, law firms:

- Handle extensive confidential information, including financial records, intellectual property, personal data, and legal strategies
- Manage financial transactions, such as real estate deals, mergers, and acquisitions
- Are privy to clients' trade secrets, intellectual property, and proprietary information
- Often represent high-profile individuals, celebrities, or companies
- Retain client data for extended periods due to legal and regulatory requirements
- Often collaborate with third-party vendors, such as court reporting services, legal research providers, or document management platforms

The trust placed in you by your clients is paramount. Holding this trove of sensitive data is an inherent and inescapable part of the legal process. Yet, it undeniably makes you a rich target for cybercriminals looking to exploit or monetise valuable information.

Cybercriminals may hack your transactions to gain unauthorised access to funds, divert payments, or manipulate financial information for financial gain. Given the sensitive nature of the information you possess, cybercriminals may also leverage the data for extortion. Threatening to expose confidential information or disrupt legal proceedings can be a powerful tool for coercing financial gain.

[1] 226 UK law firms suffered data breaches in the past year as hackers target sensitive client data, *Chaucer*, 20 January 2024." Chaucer, 26 Feb. 2024.

Case study: Supply chain risk

In November 2023, a cyber attack targeted IT provider CTS, resulting in roughly 80 law firms being affected. This incident highlights the growing risks associated with outsourcing IT capabilities and the increasing vulnerability of the digital landscape. Along with assessing their own risk exposure, businesses must perform thorough due diligence on their suppliers to ensure they are well protected against potential threats.

In this situation, a cyber policy would have covered a law firm for their own losses and any claims brought against them by third parties. It would have provided incident response support and business interruption to cover the loss of profits and increased cost of working resulting from the event.

Ensuring success

A data breach could have severe consequences, eroding trust and tarnishing the reputation you have carefully built over the years. Contrary to popular belief, cyber insurance is far from complex, and it can provide a vital safety net, covering:

- Legal expenses and potential settlements in the event of a data breach, allowing you to manage the aftermath without a significant financial burden
- Expenses related to data recovery, system restoration, and legal liabilities
- Specialist guidance, helping you navigate the complex web of regulatory requirements and avoid penalties that may arise from non-compliance
- Ransom payments, ensuring you can recover data without succumbing to the financial pressures exerted by attackers
- Business interruption, compensating you for the income lost during the downtime
- Public relations efforts to manage the fallout of a cyber-incident

Conclusion:

In an increasingly digital world, recognising the importance of protecting your practice against cyber threats is vital. Cyber insurance offers a comprehensive solution, providing financial, legal, and reputational support in the face of a cyber incident. Investing in cyber insurance is not just a precautionary measure; it's a strategic move to protect the future success and integrity of your firm.

Connect with us:

James Wall
Director, Technology and Cyber Practice

M: +44 7506 721 853
E: james_wall@ajg.com