CRC Group
Wholesale & Specialty

Why Law Firms Can Be Challenging for Cyber Insurers

Being a successful lawyer hinges in part on never underestimating your opponent. Yet many law firms have failed to heed this maxim when it comes to cybersecurity. Unfortunately, cybercriminals have devoted themselves to understanding the technology and security protocols as well as social behaviors specific to many law firms. Combining intelligence, technological skills, and keen behavioral insights, they stealthily deploy diverse methods of attack.

IT'S ALL ABOUT DATA

Apart from their vulnerability to phishing and ransomware schemes arising out of inadequate cyber security measures, it is all about data. Law firms maintain huge amounts of data - a highly confidential treasure trove of diverse but sensitive information ranging from merger and acquisition contracts, patent research, and financial statements to medical data, criminal records, and other personally identifiable information.

It is because of the quantity and particular nature of this data that law firms have been specifically targeted; many have moved expeditiously to pay the full ransom demand quietly and quickly to recover their encrypted or stolen data. If this data is exfiltrated it may be considered a data breach and threatens their clients' wellbeing, financially and emotionally, potentially leading to lawsuits arising out of the failure to protect client data, a primary duty of any law firm. As of July of 2023, it was reported that five class action lawsuits had already been filed by clients alleging their law firms had not done enough to protect against cyberattacks.[1]

By tracking payments across cryptocurrency blockchains, the company Chainanalysis discovered that a record $1.1B was lost in ransomware payments globally in 2023.[4]

©2024 CRC Insurance Services, LLC, CRC of California Insurance Services, CA Lic No 0778135. No claim to any government works or material copyrighted by third parties. Nothing in this document constitutes an offer, inducement, or contract of insurance. Financial strength and size ratings can change and should be reevaluated before coverage is bound. This material is intended for licensed insurance agency use only. This is not intended for business owner or insured use. If you are not a licensed agent please disregard this communication.

062024-1460-CRCG

WHAT ARE THE RISKS?

Phishing remains the most popular attack method deployed against law firms, enabling attackers to engage in social engineering schemes as well as launch ransomware, which can extend an extortion demand into a data breach. Public reports of data breaches at prominent law firms have become common occurrence. In April 2023, a large law firm had more than 184,000 files containing confidential data leaked on the open web. The data was exposed for a full six months before a cybercriminal found it. The data was housed on an unsecured server managed by a third-party company. Similarly, in 2017, a law firm employee fell victim to a phishing scam. The employee received an email request for personal information, including the W-2s of current and former employees. Because the email address looked legitimate, the confidential information of 859 people fell into the hands of a cybercriminal.[3] In a class action suit (later dropped) filed against another firm, the company was accused of failing to protect the personal information of more than 19,000 in a 2021 cyberattack.

The evidence speaks for itself in identifying law firms as a primary target for cyber criminals. In a 2023 American Bar Association survey, 29% of law firms reported experiencing a data breach. In their April 2023 report, Checkpoint Research revealed that one out of every 40 cyberattacks targeted a law firm.[2]

CYBER MARKETPLACE EXPECTATIONS

As a result of paying out policy limits to meet extortion demands, the cyber market for law firms has contracted significantly as many insurers have exited this class, taken significant rate increases, or will only consider very small firms for new business. As an alternative, some carriers have reduced limits, particularly ransomware sub-limits, to as low as $250,000. Others will no longer offer cybercrime as social engineering attacks, specifically involving fraudulent wire instructions, have become too frequent. Of those that still do offer the coverage, some will not cover any funds held in escrow, a significant exposure for many firms.

Regardless of revenue size, eligibility for coverage is very tight and comes down to a thorough examination of cyber security measures employed. At a minimum, firms which do not employ multi factor authentication (MFA), endpoint detection and response (EDR) and encrypted, offline backups or other security measures such as anti-phishing training may find themselves uninsurable - at least until such measures have been implemented. Law firms seeking cyber coverage routinely receive cyber security recommendations from an insurance company's cyber security team. As part of the underwriting process, this team does an initial scan to look for open ports and other vulnerabilities a threat actor can exploit. Law firms applying for coverage who are not agreeable to implementing these recommendations may find they cannot bind coverage.

According to an American Bar Association survey, 29% of respondents reported their firm had experienced a security breach in 2023.[5]

In addition to a strong cybersecurity stance, law firms would also be wise to avoid cyber exclusions or sub-limits on their lawyers professional liability (LPL) policies as they can result in an unfavorable outcome on what could otherwise provide liability coverage in a cyber claim scenario.

However, in the final analysis, none of these steps will make a law firm entirely invulnerable to a cyberattack. One of the most notorious cyberattacks against a Panama City, FL law firm, later referred to as the Panama Papers, put 11.5 million records in the hands of news outlets worldwide. Many believe it was the result of an inside attack.[3] Regardless of a law firm's security protocols, the temptation presented by a wealth of confidential information can prove overwhelming and criminals may target employees, offering them financial rewards to gain access to client data.

BOTTOM LINE

Law firms looking for cyber coverage are strongly encouraged to take their cybersecurity as seriously as possible as cybercriminals view law firms as low-hanging fruit. Cybercriminals are highly skilled and will exploit any vulnerability they can find. No set of security protocols is totally impenetrable, and cyber liability coverage should be a key part of any law firms risk management plan. Firms that take cyber security seriously by implementing robust security protocols will find the best coverage options available. Partnering with a wholesale broker knowledgeable about the cyber risks law firms face can make a difference in today's tight market. Reach out to your local CRC Group broker today for help navigating the challenging cyber marketplace for law firms.

CONTRIBUTOR

- **Mark Smith, CPCU, RPLU,** is a Senior Vice President out of the Seattle office specializing in Cyber & Technology, Errors & Omissions, Healthcare Professional, and Management Liability.

GUEST CONTRIBUTORS

AMAN ARORA

Aman Arora is an AVP, Cyber and Tech E&O Underwriting at Corvus and is based in the San Francisco Bay Area. He is a graduate of the University of Texas School of Law and UCLA.

KATIE FAIRHART

Katie Fairhart, CIC, MLIS is a Senior Business Development Specialist with Coalition.

SANDY PERDIGUERRA

Sandy Perdiguerra is Senior Vice President & West Coast Manager at At-Bay where she specializes in financial lines products. She has amassed more than 17 years of underwriting and management experience focused on cyber and technology as well as management liability and professional liability coverage.

END NOTES

1. Law Firm Cyberattacks Grow, Putting Operations in Legal Peril, Bloomberg Law, July 7, 2023. https://news.bloomberglaw.com/business-and-practice/law-firm-cyberattacks-grow-putting-operations-in-legal-peril

2. Global Cyberattacks Continue to Rise with Africa and APAC Suffering the Most, Check Point Solutions, April 27, 2023. https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise/

3. The Top 10 Legal Industry Cyber Attacks, Arctic Wolf, July 20, 2023. https://arcticwolf.com/resources/blog/top-legal-industry-cyber-attacks/

4. Ransomware Payments Hit a Record $1.1 Billion in 2023, Wired, February 7, 2024. https://www.wired.com/story/ransomware-payments-2023-breaks-record/

5. 2023 Cybersecurity Tech Report, American Bar Association, December 18, 2023. https://www.americanbar.org/groups/law_practice/resources/tech-report/2023/2023-cybersecurity-techreport/