Law firms in the cyber cross hairs - the rising stakes for law firm cyber security

By Darren L. Williams, Senior Vice President
Geoffrey K. Allen, Executive Vice President and Professional Liability Practice Leader

Law firm cyber security issues have flooded industry and mainstream publications over the last few months as the Wall Street Journal, Crain’s Chicago Business, American Lawyer and others have reported extensively on hacking attempts and incidents against the legal industry, including some of the largest law firms in the United States. In 2009, the Federal Bureau of Investigations (FBI) issued an advisory noting that law firms were targets of hackers. In 2011, the agency held meetings with a number of top law firms to highlight some of the threats, and in 2013 reiterated its message. Despite these warnings, many law firms have not adopted appropriate cyber security risk mitigation strategies, including the purchase of cyber insurance.

Unlike public companies, the announcement of breaches in the legal industry has been sporadic due to limited regulatory oversight and responsibility for notification. While The American Bar Association and some state bar associations have provided opinions and recommendations regarding assessment of data risks and the importance of protecting client information, these are only guidelines. However, following the latest breaches, such as the hacking of a number of prestige U.S. law firms for the purpose of obtaining insider trading information (https://bol.bna.com/fbi-alert-warns-of-criminals-seeking-access-to-law-firm-networks/), some regulatory oversight may be on the horizon. Law firms with responsibilities to protect data under the Health Insurance Portability and Accountability Act (HIPAA)

“Attorneys themselves and assistants are going to be the weakest point of any cybersecurity system,” said John Reed Stark, Esq., a former SEC enforcement lawyer who now runs a cyber security consulting firm in Bethesda, Maryland. “I just don’t get the sense that law firms really want to seriously engage for risk and security assessments.”
The “Panama Papers” are another issue which has received significant recent press coverage. The release of the Panama Papers puts law firms on notice that they must now also defend against threats from hacktivists. The goal of the release was not for the hackers' direct economic gain but, rather, to highlight what the hacktivist sees as an injustice by certain politicians and the elite class often represented by some of the top law firms in the world. As is now evident by the release of the Panama Papers, the exposure of these representations and details of same could lead to cyber liability claims by clients and significant reputational risk for law firms.

Given the above risks, law firms must become more diligent with respect to the adoption and implementation of appropriate cyber security strategy. The strategy is not unlike the risk management steps that law firms take in the delivery of legal services, but should include the following enhanced cyber security measures:

- Identifying data assets and the supporting systems.
- Analyzing the threat landscape against the assets and controls to mitigate the threats.
- Understanding where the firm’s data assets may sit in an attacker’s supply chain.
- Evaluating the financial impact to clients if the firm fails to prevent an attack that exposes clients’ information.
- Determining the likelihood of an attack and the cost of residual risk if an attack cannot be prevented.
- Ensure management’s commitment to effective policies and procedures and enforcement of same for all attorneys and staff.

- Conduct cyber risk training for attorneys and staff several times a year.
- Ongoing investment in cyber security technology and third-party assessments.
- A breach response plan that has been tested.
- Investigation of network security and privacy liability insurance, based on a clear understanding of the probable cost of risk and coverage under current policies such as lawyers’ professional liability insurance, to mitigate the financial consequence of a breach and provide access to breach response resources on a priority basis.
- Reviewing adequacy of coverage limits based on the prior evaluation of residual risk.

Finally, client demand has been a driving force for many firms’ decision to purchase cyber insurance. While a typical lawyers professional liability policy will likely respond to a client’s claim for a breach of their confidential information, there are a range of gaps and ambiguities that a Cyber policy covers. Important Cyber risk policy coverage for a law firm includes: extortion demands threatening release of data or harm to systems, breach of employee information, business interruption (lost income and extra expense), business information (lateral hire and merger negotiations), breach at information holder processing information for the firm under contract (e.g. eDiscovery vendor), privacy regulatory defense expenses and fines, and forensics expenses to investigate a breach. Given the developments noted above, we expect this trend to accelerate.

How Willis Towers Watson can help

The Willis Towers Watson FINEX North America Professional Services Practice is well versed in network security and privacy liability insurance for law firms, as well as professional liability, employment practices liability, management liability and outside directors’ and officers’ liability insurance.

With an international law firm clientele, FINEX has professional services teams in New York, Orange County (CA), London, Bermuda and other countries. For additional information and inquiries regarding our risk management solutions, please contact:
The observations, comments and suggestions we have made in this publication are advisory and are not intended nor should they be taken as legal advice. Please contact your own legal adviser for an analysis of your specific facts and circumstances.

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 39,000 employees in more than 120 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.