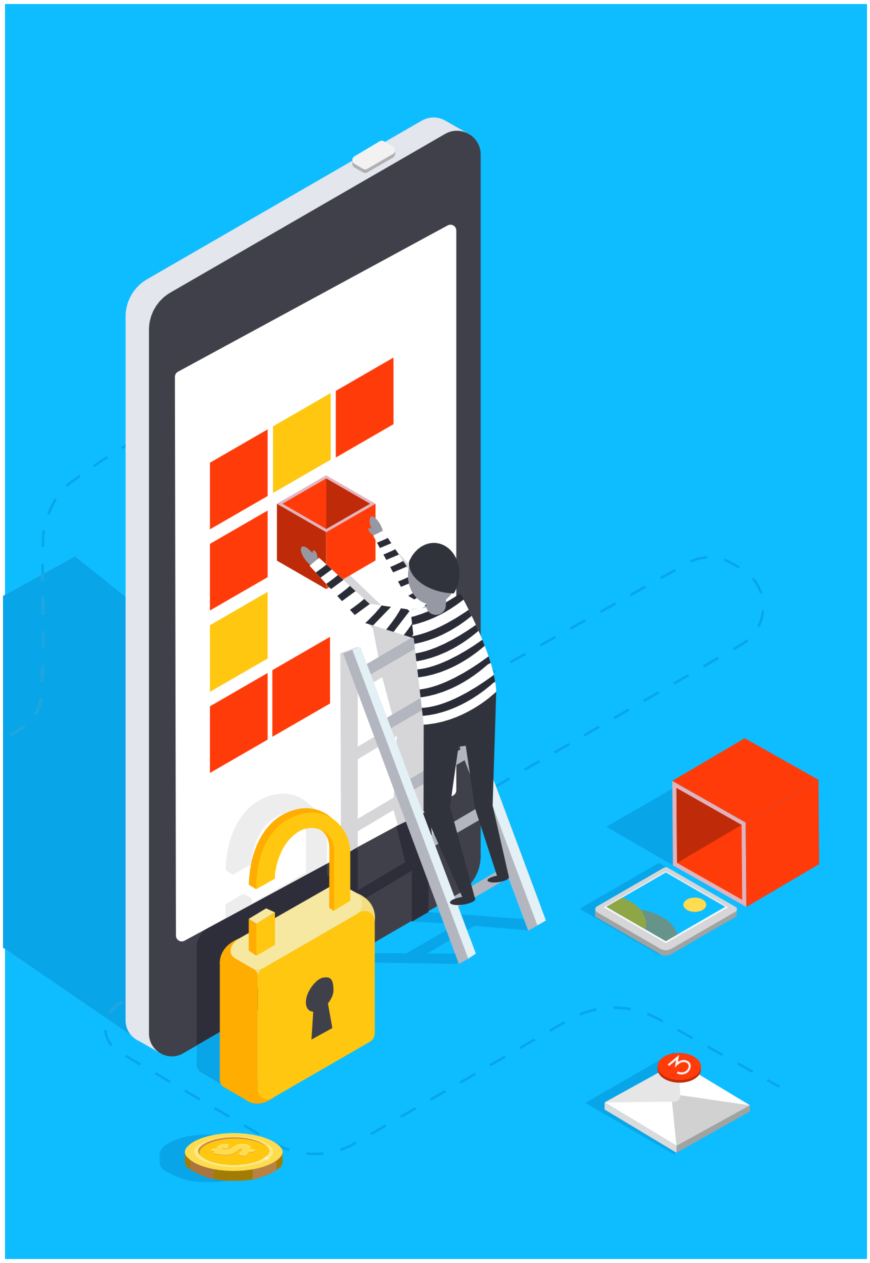
# Keeping Your Firm Out of Cybersecurity Headlines

If law firms still had doubts about the need to pay more attention to cybersecurity, the last 12 months should have dispelled them completely.

by David Levine



Ransomware, for example, was no stranger to law firms and in some cases had crippling impacts on productivity and profitability and/or resulted in litigation. Mossack Fonseca, the law firm at the center of the 2016 Panama Papers scandal, cut its global offices from 45 to six, and firm cofounder Jurgen Mossack acknowledged that the data breach had damaged the firm's credibility and bottom line. And in December 2016, the FBI and the U.S. Attorney for the Southern District of New York charged three Chinese traders with securities fraud, saying the traders had targeted multiple mergers and acquisitions law firms, broken into the systems of at least two of them and traded on stolen non public information to make millions.

"This case of cyber meets securities fraud should serve as a wake-up call for law firms around the world," said U.S. attorney Preet Bharara in a statement released about the final incident. "You are and will be targets of cyber hacking, because you have information valuable to would-be criminals."

At Ricoh we see that the legal industry is taking cybersecurity seriously as our customers increasingly ask extensive and detailed questions about our own security measures. Corporate clients are starting to audit their law firms' cybersecurity stances and pull their business if the firms fails to meet standards. For the first time some of our law firm customers are citing cybersecurity as their biggest competitive differentiator. In short, firms are realizing that good cybersecurity is not only critical to reducing business risk but also an important way to build competitive advantage.

## New Attacks and New Rules in 2017

Ransomware attacks — specifically, massive attacks such as WannaCry and Petya — dominated the headlines in the first half of 2017, and major law firms were not immune. But while ransomware made the most headlines, other types of cybercrime continued apace.

In a recent survey of 200 U.S. law firms by LOGICFORCE, 66 percent reported that they had experienced a breach of some type, with varying levels of compromise. The Ponemon Institute's 2017 Cost of Data Breach Study polled over 400 companies around the world, and all of them said they had experienced a data breach that compromised records. Notably, the category of "services," which includes law firms and legal services, experienced the largest increase in per capita cost of data breaches.

The year also saw a number of new rules come into effect that emphasize attorneys' ethical responsibility to protect client data. The New York State Department of Financial Services imposed stricter information safeguards on lawyers in that industry. The *New York Law Journal* summed up the impact of the new requirements this way: "Those firms that can meet the regulatory and client expectations for cybersecurity will get or retain the business, and those who don't, won't."

In June, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 477R detailing a lawyer's ethical obligation to protect confidential client information, examining advances in technology and ever-increasing cybersecurity threats and providing guidance on when and how to tighten security measures. These days "law enforcement discusses hacking and data loss in terms of 'when,' and not 'if,'" says the opinion, further noting that:

> *Law firms are targets for two general reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client.*

## Tips for 2018

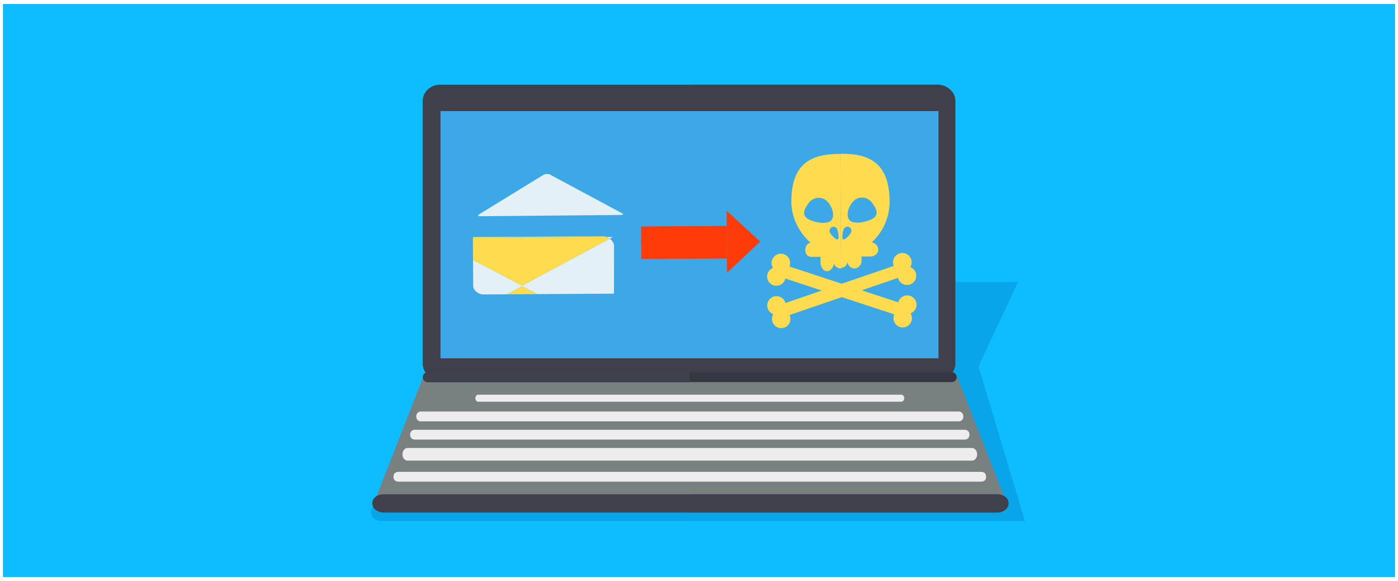
We can expect that 2018 will bring continued attacks on law firms. To make sure you are prepared, we recommend the following:

» **Hire qualified cybersecurity experts.** In the LOGICFORCE survey, only 30 percent of law firms had a credentialed chief information security officer, information security manager or similar position. Large firms can usually afford to hire their own internal security staff; smaller firms can hire managed security services providers (MSSPs) or consultants. Either way, having dedicated, qualified personnel is critical to combating threats.

» **Identify what data you have and where that data is stored.** Many firms think they know where their data is stored, only to be surprised when an audit reveals that their sensitive data is being stored in unsecured locations such as home PCs, unencrypted thumb drives or personal smartphones. As ABA Opinion 477R puts it: "The lawyer's task is complicated in a world where multiple devices may be used to communicate with or about a client and then store those communications. Each access point, and each device, should be evaluated for security compliance."

» **Recognize the value of your data.** The events of the last year leave no doubt that hackers target law firms in order to steal or hold hostage client data. The law firm's own data, including employee and financial information, can also be highly valuable. What if a hacker accessed and sold

**The very visible damage from data breaches combined with increased demands by clients for improved security makes a convincing case for investing to protect your data and your business.**



**DAVID LEVINE**
David Levine is Vice President of Information Security & CISO for Ricoh USA, Inc. Levine chairs Ricoh's Security Advisory Councils and HIPPA Board of Directors, leads Ricoh's Global Virtual Security team and is routinely engaged in customer opportunities to discuss risk and security. He holds a Bachelor of Arts degree in Information Systems with minors in Computer Science and Business from Eckerd College.

information on a case litigation strategy? Such a breach could result in the loss of both case and client, a loss potentially in the millions that could put you out of business.

» **Train all staff, from senior partners to administrative assistants, on good security practices, including how to recognize (and not click on) phishing e-mails.** The LOGICFORCE survey found that only 22 percent of law firms had a documented cybersecurity training program for employees. Only 29 percent of the firms with training programs held them at regularly scheduled intervals, and only 42 percent made them mandatory for their attorneys. Know and understand what regulations apply in your practice areas (such as the New York regulations for firms in financial services) and customize your training accordingly.

» **Use encryption wherever appropriate.** Deciding what is appropriate requires looking carefully at your data, its level of sensitivity and what type of encryption is most effective.

» **Secure new services.** Competitive pressure is driving law firms to offer new online services such as web portals and virtual private networks to meet client need for information on demand. Such services can also create new ways for hackers to break into your network and access data, so make sure that your security/risk team reviews all new services for vulnerabilities.

» **Thoroughly vet the security of third-party service providers, including cloud service providers.** Understand where they store your data, whether and how it is encrypted and what security standards and certifications the provider meets.

» **Make sure systems and software are patched and up to date.**

## Conclusion

In hindsight, 2017 may prove to be a turning point in law firm cybersecurity and become noted as the year when many firms made cybersecurity a top priority. Whatever history tells us about 2017, you can determine to significantly lower the chances of your firm making headlines in 2018. The very visible damage from data breaches combined with increased demands by clients for improved security makes a convincing case for investing to protect your data and your business. **P2P**

This article was first published in ILTA's Winter 2017 issue of *Peer to Peer* titled "2017 In Review: Successes and Lessons Learned" and is reprinted here with permission. For more information about ILTA, visit www.iltanet.org.