


CYBERSECURITY

Stopping Data Breaches in Their Tracks


Leslie A. Gordon





When sophisticated hackers engineered massive data breaches at companies like Target and Sony, cybersecurity preparedness became a priority for large companies. As corporate giants shored up their data security protection, hackers' attention turned to the next vulnerable targets: smaller businesses and professional services firms.


Law firms, in particular, are warehouses of all kinds of exploitable personal data—such as names, Social Security numbers, driver's license numbers, financial account information, medical history, salary information, and performance evaluations—of their clients, case witnesses, their own employees, and other individuals. Law firms also house other kinds of extremely sensitive information such as draft patent applications and companies' strategic plans, litigation strategy, and financial information.

Nearly 80 percent of the hundred largest U.S. law firms were hacked in 2011, according to a 2012 report by security consulting firm Mandiant. In California, data breaches grew by 600 percent in 2013, according to a 2014 report from the California attorney general. Some notable breaches involved law firms:

 In 2012, the hacker group Anonymous stole three gigabytes of sensitive files from the Virginia-based firm Puckett & Faraj and posted them online. The firm later folded.

 In 2014, it was reported that the National Security Agency and its Australian counterpart had been monitoring communications between law firm Mayer Brown and Indonesian officials that were clients of the firm.

 Redlands-based law firm Ziprick & Cramer was attacked with ransomware, a type of malware that encrypts files with decryption available only if the victim pays the malicious hackers. Malware can make its way into organizations through attachments to phishing emails.

 After filing a software piracy suit in 2010 alleging the Chinese government stole a client's intellectual property, the Los Angeles firm Gipson Hoffman & Pancione came under cyberattacks believed to have originated from China.

Security practices are part of attorneys' professional duties of competence and confidentiality, according to 2012 amendments to the American Bar Association's (ABA) Model Rules of Professional Conduct, the ABA's 2014 Cybersecurity Resolution, as well as many state ethics rules. In particular, lawyers must make reasonable efforts to prevent inadvertent disclosure of or unauthorized access to client information. "Because of the evolving nature of technology and differences in security features that are available, the attorney must ensure the steps are sufficient for each form of technology being used and must continue to monitor the efficacy of such steps," a State Bar of California opinion declared.

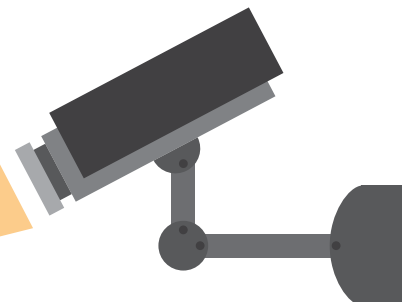
According to casualty company CNA, the average cost of a data breach in the United States as of 2013 was \$5.4 million, including crisis management services, forensics investigations, legal counsel, and breach notification expenses. Those figures don't include a data breach's reputational impact, which is particularly critical for professional service firms.

Yet attorneys and law firms are notoriously slow to adopt technology practices, particularly those related to cybersecurity. According to a 2014 survey by risk management firm Marsh, 79 percent of law firm respondents viewed cybersecurity as one of the top ten risks, yet 72 percent reported that their firm had not assessed and scaled the cost of a data breach. Forty-one percent said their firm hadn't taken measures to insure their cyberrisk.

A few years ago, the FBI stepped in and "quietly made the rounds to law firms around the country because they're a weak link in the chain," says Jones Day partner Jeff Rabkin. "Law firms have information about clients, about significant transactions, and other sensitive information, making them vulnerable to nation-state and criminal actors." Lawyers have ethical and professional obligations to maintain the secrecy of clients, but they're also less sophisticated about adopting preparedness practices, Rabkin adds. "State bars across the country now have rules about this. When law firms aren't prepared, they're really disregarding basic hygiene. A data breach can amount to malpractice."

The risks to law firms, adds Sylvia Johnson, a lawyer at Wells Fargo specializing in cybersecurity and privacy, are "very real." So to provide timely information and analysis regarding global developments in cybersecurity, privacy, and data protection law, The Bar Association of San Francisco (BASF) has launched the Cybersecurity and Privacy Law Section, which Johnson and Rabkin cochair. The group will focus on emerging technology, business practices, regulation, and litigation. "It's primarily an opportunity for information sharing and training about cybersecurity," Johnson explains. "The section will promote interaction and collaboration between public and private sectors."

Nearly **80 percent** of the hundred largest U.S. law firms were hacked in 2011[...] In California, data breaches grew by **600 percent** in 2013.



Leaders of the new section include a dynamic cross section of organizations, including lawyers practicing in big law firms, in-house at companies, at advocacy groups, and in government. As well as Johnson and Rabkin, founding attorneys of the section include Lee Freedman of Apple Inc., Katherine Tassi of Uber, Matthew Parrella from the U.S. Attorney's Office for the Northern District of California, and Google's Nicole Jones.

In addition to the professional responsibility element, cybersecurity preparedness is now an important factor in many firms' getting hired—or not—according to Johnson. For instance, “being a very large banking organization with multiple lines of business, Wells Fargo is very highly regulated—by the Office of the Comptroller of the Currency (OCC), the Federal Reserve—and is very concerned about the security of customer and employee data. Third parties we do business with are expected to adhere to high standards.” As a result, there's a “stringent process” for selecting the bank's outside counsel. “One factor is information security. We have a team of compliance people who do a complete assessment.”

For law firms that want to shore up their preparedness, Rabkin has several pieces of advice. “First, for any professional service company—this is like cybersecurity 101—you must have executive-level involvement,” he says. “This is not something that just an IT person deals with. Executives must empower a culture of security throughout the organization.”

To that end, training employees is essential. “Here's the classic scenario,” Rabkin says, “USB drives are scattered in a parking lot. Workers find them and, thinking they're doing a

good deed, plug them in so they can see whose they are and return them. But that's a classic way to install malware.”

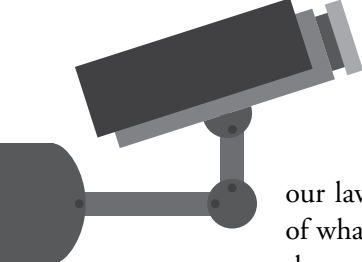
Similarly, because many law firms existed in the pre-Internet era, their IT “may not be fully mapped,” Rabkin says. “Many firms don't even know what data they have or where they have it. They must figure that out and get rid of what they don't need.” Law firms should also closely evaluate their business partners and vendors because everyone from e-discovery firms to copying companies to IT to other nonlegal services can be “vectors” of cybersecurity problems.

Because breaches are inevitable, according to Rabkin, law firms must not only have cyber-breach insurance but also a plan and a team in place for that eventuality. “It's not enough to focus on prevention. You can't devise your plan after it's already a problem—you can't build an airplane in the air,” he says. So Rabkin recommends consulting experts—such as outside counsel, security vendors, and law enforcement, including the local FBI—to devise an incident response plan. “These kinds of things always happen on a Friday night or on a holiday. You don't want to be searching for a team then.”

So far, law firms' cybersecurity efforts have largely been reactive, notes Daniel Hutchinson, a consumer privacy lawyer at Lieff Cabraser Heimann & Bernstein, who is co-vice chair of the new BASF section. “So victims of data breaches then often have to shuffle to figure out what should be done.”

Because there's been “far less guidance” in this area than necessary, BASF's Cybersecurity and Privacy Law Section fulfills a distinct need in the professional community, Hutchinson adds. “There are so many implications to cybersecurity. We'll provide CLEs with advice and information from experts about the way we should operate

79 percent of law firm respondents viewed cybersecurity as one of the top ten risks, yet **72 percent** reported that their firm had not assessed and scaled the cost of a data breach.



our law firms. It'll help firms to be aware of what some of the potential issues are so they can see how it'll impact them or not."

Importantly, law firms must continually reevaluate their cybersecurity preparedness. "Given the state of technology, the issues today are different from the issues there will be five years down the road," Hutchinson says. "Ten years ago, we were looking at physical computers and servers inside four walls. Now, people are working on devices."

Indeed, the most common breach experienced by law firms centers on the loss or theft of laptops, drives, phones, and tablets, whether owned by the firm or personally owned by the lawyer or a firm employee. According to CNA claim data, a lost or stolen laptop or device is the most frequent cause of a data breach claim.

"Many lawyers and law firm employees use their own devices for client emails and documents," says Jennifer Lynch of the Electronic Frontier Foundation (EFF). "When a device is left behind somewhere, it can be hacked into very easily." If the device contained files or access to files with personally identifiable or other proprietary information and it wasn't encrypted, the firm is vulnerable to a breach.

Similarly, lawyers working over open, unsecured Wi-Fi systems like those at airports, hotels, and cafes pose another distinct cybersecurity risk. Fortunately, fixes are relatively simple, Lynch says. For instance, lawyers can use the firm's virtual private network, which is harder to intercept. And the firm can invest in software that remotely wipes a lost device. The section's April 2016 CLE meeting will cover this BYOD (bring your own device) topic.

Given the proliferation of technology in the law, all kinds of firms—large, small, and solo—must take steps to protect themselves, according to Rabkin. "The bad guys are

shifting their focus from large organizations, like financial institutions, and are increasingly targeting mid- [to] small-sized businesses," he says. "You need to be serious about this even if you're a solo practitioner."

While some might argue that it's cost prohibitive for small firms to prepare for cyberattacks, Wells Fargo's Johnson disagrees. "A large firm has tremendous complexity, and that's a cost challenge," she says. "But small firms have less complexity, so it's easier to meet the requirement." Rabkin adds, "It's not prohibitively expensive, especially when you think of the expense of a serious incident. There's no excuse for having client data out there that's not encrypted, for example."

Furthermore, firms shouldn't assume that cybersecurity threats will come only from outsiders, Hutchinson cautions. "Just like with regular crime, you're more likely to be a victim from someone you know," such as a fired employee or someone else about to leave the firm. And that can happen at a firm of any size.

According to the EFF's Lynch, "You have to know what your threat model is and design a security system based on that. If your firm is dealing with extrasensitive data, that will need more protection than, say, a random email."

On January 20, 2016, the Cybersecurity and Privacy Law Section's first CLE will cover the "Internet of Things," addressing risks of networked devices such as the Nest thermostat, self-driving cars, networked light bulbs, and heart pumps with remote access, according to Rabkin. "These everyday devices generate a host of security and legal issues."

*A former lawyer, Leslie A. Gordon is a freelance journalist living in San Francisco. She is the author of *Cheer: A Novel and Heads or Tails*, both available on Amazon. She can be reached at leslie.gordon@stanfordalumni.org.*