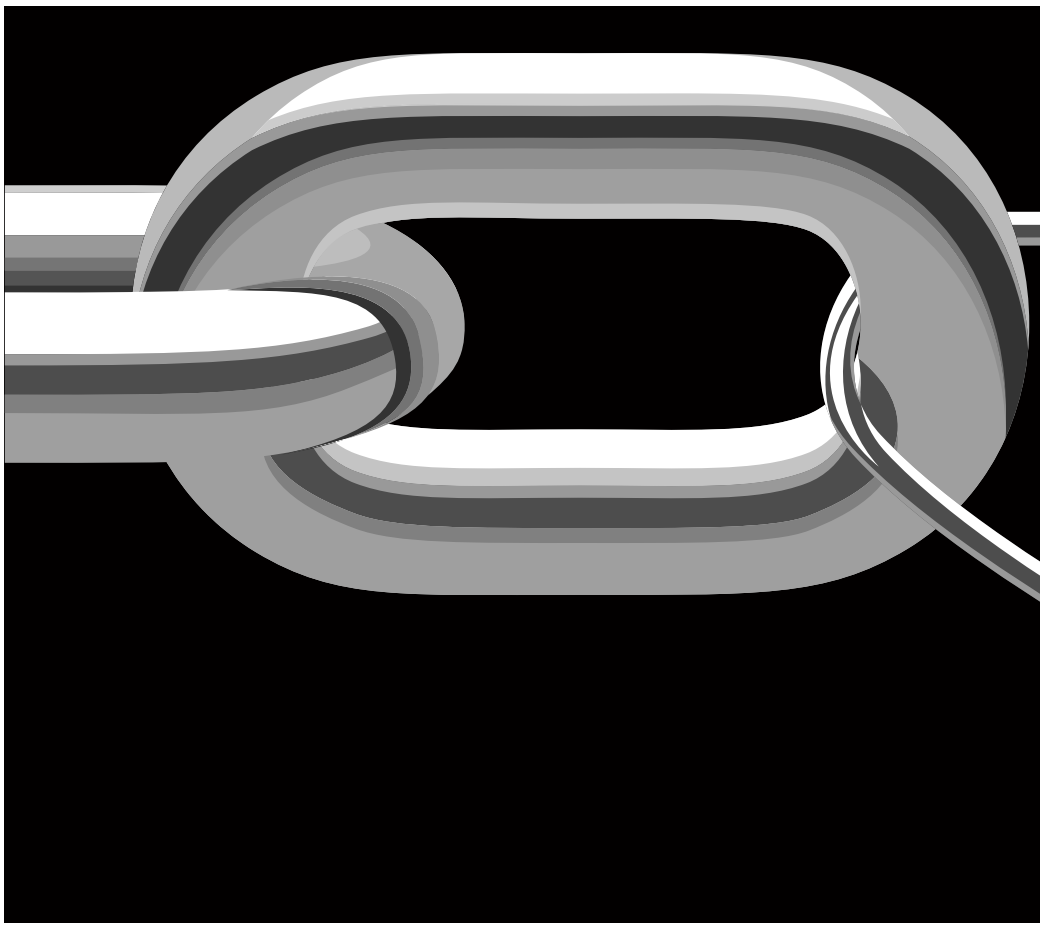
Hacks, Files, and Ethical Gapes



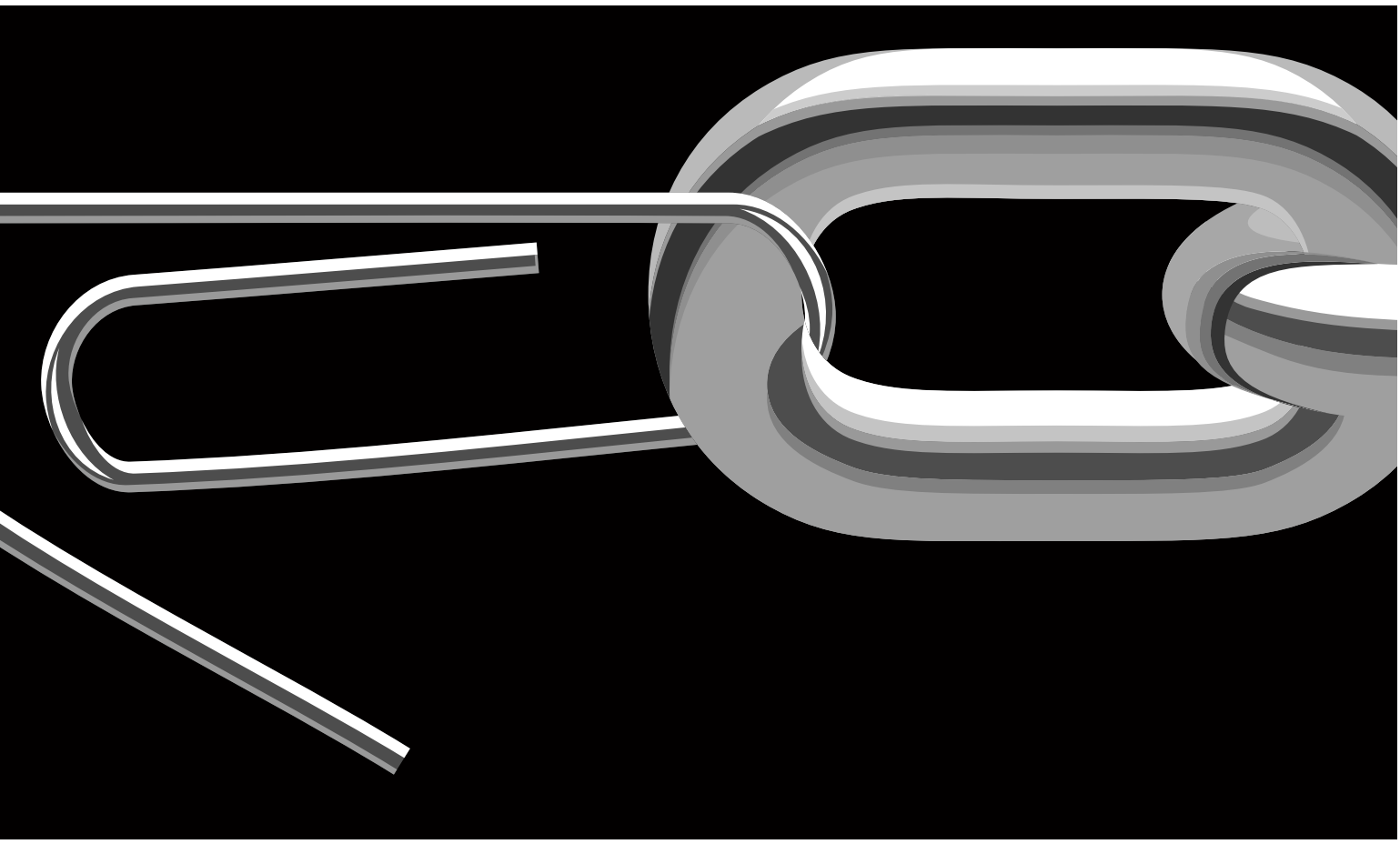
Attorneys' Liability for Data Breaches

By Sean C. Griffin

Most companies have rigid IT policies and safeguards imposed by their industries; attorneys lag behind, making them the weak link in the data security chain.

Alice Assistant had always wanted to go to Bermuda. She'd heard about the pink sand, which sounded lovely, and the shopping, which sounded even better. The thing was, flights and hotels weren't cheap, so she wasn't sure she'd

■ Sean C. Griffin practices in Dykema Gossett PLLC's Washington, D.C., office, where he focuses on commercial litigation, including professional malpractice defense. In addition to litigating cases in state and federal courts around the country, he helps clients respond to subpoenas regarding anti-corruption enforcement, False Claims Act violations, and allegations of securities law violations. Mr. Griffin also regularly counsels clients in the areas of information security and data privacy, and he is an active speaker in this area. Before joining Dykema, he served in the U.S. Department of Justice, Civil Division, where he handled commercial litigation trials and appeals.



ever make it—at least not on the salary that her law firm, Shudda Nown & Better, was—.

Hold on. Right under another e-mail entitled "Bigg/Dollas merger," she saw an e-mail entitled "Cheap Bermuda Fares." After all the time that she had put in on the Bigg/Dollas merger, this was just what the doctor ordered. She clicked the link, then sighed. The website contained a bunch of misspelled words with some garish color scheme. Obviously a scam. Alice closed the window and wished the scammers better luck next time.

The scammers didn't need better luck, though. They had Alice, who, by clicking their link, gave the hackers access to Shudda Nown & Better's system. The scammers didn't spend much time looking around. They knew exactly what they wanted, and they found it in a folder helpfully labeled "Bigg/Dollas Merger."

The merger collapsed quickly after that.

A few days later, E. Larry Queen sat in the office of Lana M. Parterre, Shudda Nown & Better's managing partner. He tried to offer words of comfort.

"This sort of thing happens more than you think."

As an example, Queen told Lana about an incident in September 2010, when China-based hackers, determined to derail an Australian company's acquisition, attacked one computer network after another, trying to find a weak point. Eventually, they found it—not in the Australian company, or in the potential target, but in the law firms handling the deal. The hackers hit seven law firms, culling their clients' most sensitive information and other client confidences. Ultimately, the deal fell apart. *China-Based Hackers Target Law Firms to Get Secret Deal Data*, Bloomberg News Service, Jan. 31, 2012.

Such attacks have become increasingly common. Whereas companies have become more sophisticated and vigilant about protecting their and their customers' confidential information, attorneys lag behind, making them the weak link in the data security chain. A recent ABA survey found that 25 percent of law firms with at least 100 attorneys have experienced a breach. *1 In 4 Law Firms Are Victims Of A Data Breach*, Law360 (Sept. 22, 2015). Cravath Swaine & Moore LLP and Weil Gotshal & Manges LLP were reportedly among the firms hacked in early 2016. Based on the ABA survey, other, lesser known firms likely suffered the same fate.

Why Law Firms?

Lana became agitated. "Why us? What did we do to deserve this? We're just innocent attorneys—practically bystanders!"

"Lana," Queen said. "You might be underselling both your attractiveness as a hacking target and your culpability."

"What do you mean?"

Queen explained the hacker's mindset. It was all about efficiency. Most companies have rigid IT policies and safeguards imposed by their industries, implemented by knowledgeable IT personnel, and enforced by a relatively powerful manage-

ment. This means that hacking most companies poses a substantial challenge.

In contrast, most law firms are run by attorneys, who face no industry standards for cybersecurity. Further, the management structure of most law firms leaves key matters of cybersecurity to their lawyers' discretion, and those lawyers are often ignorant of cybersecurity risks and unwilling to learn. Attorneys frequently require access to their clients' information at any time and in any context, and this demand can impose vulnerability upon a firm's data security efforts. Busy, distracted lawyers also ignore important security notices, which also expose firm data to hackers. Other attorneys resist security efforts in the name of convenience; an estimate from 2012 stated that 26 percent of law firms do not require simple passwords for wireless e-mail devices. *E.g.*, Jeffrey Brandt, *When Good Enough—Isn't*, Legal IT Professionals (Mar. 28, 2012), http://www.legalitprofessionals.com. All this makes the typical law firm's data security weak. Forty-seven percent of respondents to the ABA survey said that their firms have no response plan to address a data privacy breach, and another 25 percent did not know if their firms had plans. *Id*. More than half of the attorneys surveyed said that their firms did not have a dedicated chief information security officer or other staff member charged with data security. *Id*. Attackers seeking information about a particular company may find it easier to find out the identity of the law firms representing the company and try to attack the law firms' systems rather than attacking the company's systems directly. Law firms often employ fewer security resources than their clients, with less understanding of and appreciation for cyber risk. *See generally* Drew Simshaw and Stephen Wu, "Ethics and Cybersecurity, Obligations to Protect Client Data," (Nat'l Symposium on Technology in Labor and Employment Law, Mar. 15–17, 2015), *available at* http://www.americanbar.org/content/dam/aba/events/labor_law/2015/march/tech/wu_cybersecurity.authcheckdam.pdf.

In addition to the comparative weakness of a typical firm's data security, a hack against a law firm may be more time- and cost-efficient than hacking the company directly.

In addition to the comparative weakness of a typical firm's data security, a hack against a law firm may be more time- and cost-efficient than hacking the company directly. First, lawyers are a treasure trove of information. Lawyers usually become involved in their clients' most important business matters, meaning that hackers may not need to sift through voluminous data to find the more valuable information. Moreover, a lawyer's knack for identifying and segregating useful information may work to the hackers' advantage; the hackers can find the most relevant information helpfully organized for the taking. Simshaw and Wu, *supra*, at 4; *E.g.,* David Mandell and Karla Schaffer, *The New Law Firm Challenge: Confronting the Rise of Cyber Attacks and Preventing Enhanced Liability*, LawPracticeToday (Mar. 2012), http://www.lawpracticetoday.org/ (then navigate to archives); Michael McNerney and Emilian Papadopoulos, *Hacker's Delight: Law Firm Risk and Liability in the Cyber Age*, 62 Am. U. L. Rev. 1243–72 (2013).

Additionally, law firms have information on their corporate clients' employees, including medical information, financial information, and other data useful to hackers. This information is subject to a host of regulatory protections, including HIPAA and the Health Information Technology for Economic and Clinical Health (HITECH) Act (health information), the Gramm-Leach-Bliley Act (GLBA) (financial institutions), the Family Educational Rights and Privacy Act (FERPA) (education), the Children's Online Privacy Protection Act (COPPA) (online minors), and a wide variety of state privacy and consumer protection laws. With this information, a business rival can outmaneuver a competitor, or a hacker can blackmail an individual from half a world away. As the FBI recently warned law firms, "Hackers see attorneys as a back door to the valuable data of their corporate clients." Bill Gardner and Valerie Thomas, *Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats* 27 (2014).

The benefits are not limited to a firm's clients. Through discovery on their clients' behalf, law firms have access not only to their clients' confidential information, but often the confidential information from their clients' competitors, as well. Thus, a hack against a law firm can offer economies of scale for hackers—not unlike buying in bulk at a big-box discount store.

From the clients' perspective, this is inexcusable. Practically, the consequences are obvious; no client spends money fortifying its computer defenses only to hand its data to a vendor with the cyber equivalent of an unlocked door.

Where Do Threats Originate?

"Fine," Lana said. "I see what makes us so appealing. But I'm not paying you to make me feel badly. I'm paying you to help us figure out how this happened."

"It could be any of a number of things," Queen said.

"Like what?"

Threats to law firms may arise from a number of sources. For instance, law firms may fall victim to an inside job. Disgruntled employees might take out their job dissatisfaction on a company, and insufficiently supervised contractors may seek more financial gain than the firm offers legitimately. For instance, in 2001, a paralegal at a New York firm downloaded a copy of a trial plan from his firm's computer system and tried to sell the plan to the opposing counsel for $2 million. In a possible demonstration of why the firm may not have highly valued his services, the paralegal ended up making the sale to an undercover FBI agent. He eventually pleaded guilty to Computer Fraud and Abuse Act violations, wire fraud, and related charges. Simshaw and Wu, *supra*, at 4.

State-sponsored attacks can also pose security threats. State actors may be motivated by economic espionage, terrorism, or politics. Non-state "hacktivists" may hope to achieve a political objective through attacks. Terrorists may cyberattack law firms' security both for profit and to terrorize their victims directly. And business

competitors sometimes engage in corporate espionage for their own ends. *Id.* at 4.

Finally, a law firm can fall victim to a phishing attack, such as the trick that Alice fell for. Given the number of personnel with virtually unrestricted access to computers and the internet, and the temptation to roam the internet when bored, it is inevitable that someone in a law firm will unwisely click on a dubious link or visit a suspicious website. These visits can often expose a firm's data much more effectively than an outside hack.

What Are the Consequences?

"Great," Lana said. "I get the idea. How much damage are we looking at? I assume that we've already lost BiggCorp as our client, and we can say goodbye to BiggCorp paying our fees for the past 60 days. But I suppose that's the worst of it, right?"

Queen winced. He could think of many more unpleasant consequences.

For example, in March 2016, the Panamanian law firm Mossack Fonseca found itself the victim of a hack that published its clients' confidential information worldwide in a story knows as the "Panama Papers" leak. BBC News, *Panama Papers Q & A: What Is the Scandal About?* (Apr. 6, 2016), http://www.bbc.com/news/world-35954224. The 11.5 million documents posted online contained information about more than 214,000 offshore companies that Mossack Fonseca compiled. "We are amazed that nobody has said: 'Hey, a crime has been committed here,'" Mr. Fonseca, one of the Mossack's founding partners, said recently. BBC News, *Panama Papers: Leak Firm Mossack Fonseca 'Victim of Hack'* (Apr. 6, 2016), http://www.bbc.com/news/world-latin-america-35975503.

Be careful what you wish for. Soon after Mr. Fonseca's lament, the International Consortium of Investigative Journalists reviewed the Panama Papers and reported various instances where it appeared that Mossack Fonseca had backdated, otherwise altered, or destroyed documents to conceal its involvement with certain individuals or to escape liability.

The Panama Papers have sparked investigations of Mossack Fonseca's clients in 32 countries as of this writing. Each of those clients will be looking to determine how much of their legal expenses Mossack Fonseca can be forced to bear as a result of its inability to keep their information confidential.

Further, Mossack Fonseca itself can expect to be involved in these investigations for the foreseeable future. Its attorneys will be called as witnesses in various civil and criminal proceedings around the world, and the firm itself has been sued civilly in the United States, as well. These proceedings will incur legal costs that promise to last for years.

The Panama Papers leak shows that an organization that suffers a data breach could face serious consequences. Those consequences include government investigations, internal investigation costs, and private lawsuits from customers and shareholders.

How Do Firms and Attorneys Fulfill Their Ethical Duties?

Not only must a law firm that has suffered a breach worry about a private lawsuit, but it must worry about its ethical obligations as well. Following state ethical rules, ABA Model Rule 1.6(c) requires a lawyer to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." ABA Model Rule 1.15 provides that "property shall be identified as such and appropriately safeguarded." In 2012, the American Bar Association amended its rules to provide that lawyers "should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*…." ABA Model Rule 1.1 cmt. 6 (emphasis added). ABA Model Rule 1.6 Part (c) now says that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Comment 18 to that rule now elaborates that "[f]actors to be considered in determining the reasonableness of the lawyer's efforts" include the following:

> the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (*e.g.*, by making a device or important piece of software excessively difficult to use).

ABA Model Rule 1.6 cmt. 18.

A growing number of states have signed onto this amendment, including Arizona, Arkansas, Connecticut, Delaware, Idaho, Kansas, Massachusetts, Minnesota, New Mexico, North Carolina, Ohio, Pennsylvania, West Virginia, and Wyoming. Recently, Florida amended its Rule 6-10.3 to require attorneys to complete three hours of an approved technology program over a three-year period. The State Bar of California has issued Formal Opinion Interim No. 11-0004, which provides that "[m]aintaining learning and skill consistent with an attorney's duty of competence includes 'keeping abreast of changes in the law and its practice, including the benefits and risks associated with technology.'" *See also* N.H. Bar Advisory Op. 2012-13/4 ("Competent lawyers must have a basic understanding of the technologies they use. Furthermore, as technology, the regulatory framework, and privacy laws keep changing, lawyers should keep abreast of these changes."). Additionally, state ethics board opinions regarding a lawyer's duty to secure the lawyer's IT systems and client data—including decisions from California, Washington, and Arizona—make clear that a firm's failure to secure its IT systems properly could be seen as malpractice.

Along the same lines, the State Bar of California issued an opinion regarding an attorney's duty to keep client information confidential in a setting with which most attorneys are intimately familiar: the local coffee shop. An attorney asked the state bar whether he could access his nearby coffee shop's public Wi-Fi connection to conduct legal research and e-mail his clients. The state bar noted that information on a public Wi-Fi connection could be seen or intercepted. Due to this lack of security, the State Bar of California said:

> Attorney risks violating his duties of confidentiality and competence in using the wireless connection at the coffee shop to work on Client's matter unless he takes appropriate precautions, such as using a combination of file encryption, encryption of wireless transmissions and a personal firewall. Depending on the sensitivity of the matter, Attorney may need to avoid using the public wireless connection entirely or notify Client of possible risks attendant to his use of the public wireless connection, in-

cluding potential disclosure of confidential information and possible waiver of attorney-client privilege or work product protections, and seek her informed consent to do so.… 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.

Cal. Bar Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. No. 2010-179, at 7.

With this increasingly accepted standard in effect, it will be easier than ever for plaintiffs' counsel to hold an attorney liable for data breaches.

Data security also implicates an attorney's duty of competence. Ethical rules nationwide require attorneys to represent their clients competently, and many states impose continuing education requirements to compel their attorneys to maintain their competence: "Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." ABA Model Rule 1.1. Similarly, Florida recently amended its competence rule (Rule 4-1.1) to mandate the acquisition and maintenance of "an understanding of the risks and benefits associated with the use of technology."

Given the information that attorneys hold, and the technical expertise required to keep it safe, an attorney must demonstrate a degree of technical competence to fulfill the duty to keep the client's information confidential. This may require getting outside technical expertise. Jill Roads and Vincent Polley *et al.*, *The ABA Cybersecurity Handbook* 66 (ABA 2013).

Lawyers cannot easily delegate this responsibility. Attorneys have the duty to supervise subordinates and third parties, and those third parties include technical consultants and cloud-computing solution companies. For example, in 2013, an Ohio opinion noted that lawyers may use cloud services if they competently select an appropriate vendor, preserve confidentiality, and safeguard client property; provide reasonable supervision of cloud vendors; and communicate with the client as appropriate. Ohio Bar Ass'n Informal Advisory Op. 2013-03; *see also* Florida Rule of Professional Responsibility 4.1-1. If a data breach occurs through data held by a law firm's vendor, the law firm may be held legally and ethically responsible for any negligence in the breach.

With this increasingly accepted standard in effect, it will be easier than ever for plaintiffs' counsel to hold an attorney liable for data breaches. With 46 states and three U.S. territories having enacted breach notification requirements, law firms cannot hope to escape responsibility by failing to disclose an incident. Further, these breach notification requirements often require notice to law enforcement, civil or criminal penalties, and private causes of action.

Can the Government Intervene?

Lana sighed. "The only thing that could make this worse is if the government were to get involved." Lana stopped, waiting for Queen to assure her that such a thing could never happen. She kept waiting. Then she sighed again.

State governments have eagerly pursued private individuals for data breaches. Recently, the Trump Hotel Collection company agreed to pay $50,000 and remediate its data security after data breaches in May 2014 exposed over 70,000 credit card numbers and other personal data. According to New York's Attorney General's office, which prosecuted the matter, the hotel chain knew by June 2015 that hotels in New York City, Miami, Chicago, Honolulu, Las Vegas, and Toronto had been compromised, yet it failed to notify customers for four months, which violated New York notification laws.

The federal government has also taken an increased interest in data security. In 2015, the Third Circuit held that the Federal Trade Commission (FTC) had the authority to fine Wyndham Hotels for its repeated failures to protect its customers' data. *FTC v. Wyndham Worldwide Corporation*, No. 14-3514 (3d Cir. Aug. 24, 2015). Essentially, the Third Circuit held that Wyndham engaged in "unfair" cybersecurity practices that "unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft." These practices included failing to use firewalls, storing unencrypted payment-card information, not fixing known security vulnerabilities on the company's servers, not changing the default user IDs and passwords for those servers, and not requiring complex, difficult-to-guess passwords. *Id*. at 8–10. As a result of these failures, the FTC alleged, Wyndham exposed its clients to three cybersecurity attacks that compromised customer payment data, payment-card account numbers, and other customer data.

The FTC asserted jurisdiction over Wyndham's actions through the Federal Trade Commission Act of 1914 (FTCA), which outlaws "unfair methods of competition in commerce." 15 U.S.C. §45(a). Wyndham alleged that the FTCA did not grant the FTC jurisdiction, but the Third Circuit was unconvinced. As that court remarked:

> A company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business.

Id. at 17.

Given the FTC's successful assertion of jurisdiction over hotels, there exists no immediately apparent reason why it would not enjoy similar success if it turned its attention to a law firm that suffered a similar cybersecurity breach. Just as Wyndham allegedly "published a privacy policy to attract customers," law firms promise to keep their clients' information confidential, both explicitly and implicitly: explicitly through their assurances, and implicitly through the confidentiality rules that govern all attorneys.

The U.S. Securities and Exchange Commission (SEC) may also join the action. In September 2015, the SEC's Office of Compliance Inspections and Examinations (OCIE) published a Risk Alert notifying

financial services firms of their responsibility to protect customer data. Of particular interest to law firms is the OCIE's focus on "Vendor Management."

> Some of the largest data breaches over the last few years may have resulted from the hacking of third party vendor platforms. As a result, examiners may focus on firm practices and controls related to vendor management, such as due diligence with regard to vendor selection, monitoring and oversight of vendors, and contract terms. Examiners may assess how vendor relationships are considered as part of the firm's ongoing risk assessment process as well as how the firm determines the appropriate level of due diligence to conduct on a vendor.

National Exam Prog., Office of Compliance Inspections and Examinations, *Risk Alert: OCIE's 2015 Cybersecurity National Examination Initiative* 2, Vol. IV, Issue 8 (Sept. 15, 2015).

Thus, the federal government is pressuring clients to ensure that their vendors—including their attorneys—comply with all appropriate data security measures.

The federal government may also become involved in setting standards for the duty of care in the cybersecurity arena. In February 2013, President Obama issued an executive order, which, among other things, expanded public-private information sharing and tasked the Department of Commerce's National Institute of Standards and Technology's (NIST) with establishing a voluntary "Cybersecurity Framework" comprised partly of private-sector best practices that companies could adopt to better secure critical infrastructure. Scott J. Shackelford *et al.*, *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 Tex. Int'l L.J. 305, 308 (2015). Given that federal law already requires federal agencies to comply with NIST cybersecurity standards, and given that courts will look to NIST to derive or impose a standard of care for private actors as well, there exists a strong possibility that the framework could set the standard of care for cybersecurity in the private sector from a liability perspective. *See* 40 U.S.C.A. §§11331(a)(1), 11331(b)(2)(A)–(B) (2000); 44 U.S.C.A. §3544(b)(2)(D)(ii) (Supp. 2005) (requiring agency IT security plans to comply with NIST guidance); *United States v. Cotterman*, 709 F.3d 952, 969 (9th Cir. 2013) (citing NIST standards with respect to individuals security protocols); *United States v. Righter*, No. 4:11CR3019, 2011 WL 2489949, at *2 (D. Neb. May 19, 2011), *report and recommendation adopted*, No. 4:11CR3019, 2011 WL 2470673 (D. Neb. June 21, 2011) (citing NIST standards).

Law firms have so far taken a lax attitude toward their data security, but that attitude must change. Cybersecurity threats are increasing, and the federal government is asserting its jurisdiction over private entities that do not properly secure their customers' data. A firm that does not meet its clients' data security expectations may find that it's losing clients, facing a malpractice suit, fighting an ethics investigation, and at the wrong end of a government enforcement action—all while paying another firm to defend it. It's a situation in which no firm wants to find itself, and one that every firm should take every effort to avoid.