BLAMING THE VICTIM: HOW GETTING HACKED CAN LEAD TO LIABILITY

Sean C. Griffin

In September 2010, 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. They hit seven law firms, culling their clients' most sensitive information and other client confidences. "China-Based Hackers Target Law Firms to Get Secret Deal Data," Bloomberg News Service, January 31, 2012.

Such attacks are becoming increasingly common. Whereas companies have become more sophisticated and vigilant about protecting their and their customers' confidential, attorneys lag behind, making them the weak link in the data security chain. A 2017 ABA survey reported that 22 percent of law firms experienced a cyberattack or data breach, which represented a 14 percent increase from 2016. ABA 2017 Legal Technology Survey. A 2015 ABA survey showed that 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. "1 In 4 Law Firms Are Victims Of A Data Breach," *Law360*, September 22, 2015. 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.*

Although the link is weak, hackers see numerous benefits. From their confidential relationship with their clients, attorneys have inside details on patents, mergers, medical information, and other personal information. This information is subject to a host of regulatory protections, including HIPAA (health information), GLBA (financial institutions), FERPA (education), 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. The right details can blackmail people and outflank businesses. As the FBI 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 (2014) at 27.

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.

Moreover, an attorney's neglect in this regard can also cause the client legal consequences. 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 . . . ." Model Rule 1.1 cmt. 6. 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. Additionally, 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 New Hampshire State Bar Advisory Opinion @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.").

With this increasingly accepted standard in effect, it will be easier than ever for plaintiffs' counsel to hold an attorney liable for data breaches. *See, e.g., Jason Shore and Coinabul, LLC v. Johnson & Bell, Ltd.,* Case No. 16-cv-4363 (N.D. Ill. filed April 16, 2016) (complaint against law firm for failure to safeguard data). With 46 states and three US territories having enacted breach notification requirements, law firms cannot hope to escape responsibility by failing to disclose an incident.

Such neglect may also trigger government action. Recently, the Third Circuit held that the Federal Trade Commission 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., August 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, 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.

The FTC has used its authority pursuant to *Wyndham* to prosecute other companies that have suffered data breaches. In December 2016, the website Ashley Madison agreed to a settlement based on its inadequate security protocols, which allowed hackers access to its customers' databases. Similarly, in April 2018, Uber agreed to a settlement for its failure to disclose a significant consumer data breaches in 2014 and 2016.

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 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," wherein the OCIE noted:

> 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 Program Risk Alert by the Office of Compliance Inspections and Examinations, Volume IV, Issue 8, September 15, 2015 at 2. Thus, the federal government is pressuring clients to ensure that their vendors – including their attorneys – are complying with all appropriate data security measures.

The SEC emphasized this point in February 2018, when it issued a Commission Statement and Guidance on Public Company Cybersecurity Disclosures (2018 Guidance). The 2018 Guidance applies general security law to provide guidelines on when the SEC believes a publicly traded company should disclose cybersecurity risks and incidents. These guidelines depend on whether the occurrence could be considered "material" and the risk factors relating to such occurrences (including the probability of an occurrence and the potential magnitude of cybersecurity incidents). The SEC also noted that the company has a duty to update and correct any cybersecurity disclosures.

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 that, 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, JD, PhD 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). NIST published the draft version 1.1 of the Framework on January 10, 2017.

On May 11, 2017, President Trump banished any thought that he would change course on cybersecurity. That day, he issued a "Presidential Executive Order on Strengthening the

Cybersecurity of Federal Networks and Critical Infrastructure" that closely followed and built upon President Obama's executive order, thus signaling that President Obama's cybersecurity initiative would proceed unabated. Indeed, on May 15, 2017, NIST published its initial analysis of the responses it received to its request for comments, and the response seems generally positive.

Defense contractors generally must comply with certain NIST protocols. 48 C.F.R. 225.204-7012 (requiring contractor implementation of NIST Special Publication 800-171). The Department of Education has been considering a similar requirement for a while. Dear Colleague Letter, July 1, 2016, DCL ID: GEN-16-12. 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).

State ethics rules also impose cybersecurity duties upon attorneys. 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 1.1 requires attorneys to "provide competent representation to a client," which requires "the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." ABA Model Rule 1.15 provides that "property shall be identified as such and appropriately safeguarded." Additionally, state ethics boards regarding a lawyer's duty to secure their IT systems and client data – including decisions from California, Washington, and Arizona, make clear that a firm's failure to properly secure its IT systems could be seen as malpractice.

Attorneys 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. Outside or in-house counsel that do not meet their clients' data security expectations may find itself losing clients, at the wrong end of a government enforcement action, or both.