LJN LAW JOURNAL NEWSLETTERS

Internet Law & Strategy®

An ALM Publication

Volume 10, Number 8 • August 2012

Law Firms and Cyber Security

A Titanic Risk

By Karl G. Nelson and Michael D. Y. Sukenik

One hundred years ago, the "unsinkable" Titanic steamed headlong in the dark into a largely unseen iceberg floating in the North Atlantic shipping lanes, resulting in one of the most infamous commercial disasters in history. Just as those responsible for the Titanic were lulled into a false sense of confidence in the vessel's impenetrability, many law firms today similarly steam along with a false sense of security that the cybercrime lurking in today's electronic channels of commerce does not pose a potentially critical threat. Taking a lesson from history, firms would be well-served by a blunt assessment of the cyber security risks that surround them and whether course corrections could avert a modern-day commercial disaster.

Law Firms at Risk

In fact, in the evolving world of cybercrime, hackers, their targets, and the methods they employ are changing in ways that put law firms and other professional service providers increasingly at risk. Firms that previously took comfort in the relative absence of exploits targeting the legal industry do so today with the same misplaced confidence that doomed the Titanic. Firms are on the new frontier of cybercrime, and the prudent ones will acknowledge and prepare for this growing risk.

Converging Trends

The past decade has witnessed an evolution in the nature of cybercrime. In the past, hackers typically focused on stealing financial data from individuals and businesses in order to quickly convert the purloined information into direct financial gain, typically through fraud. By contrast, modern cybercrime has expanded to target other sources of sensitive information in pursuit of goals beyond immediate profit. With this change in focus, hackers have not overlooked the increasingly crucial and intertwined role law firms play in business. Lawyers advise regarding sensitive business and political issues, conduct due diligence, engage in intensive discovery, negotiate and close transactions, and litigate major disputes. All the while, they enjoy profound access to the most sensitive — and often most potentially damaging — information possessed by their clients. That information can include financial data, trade secrets, intellectual property, business strategies, and candid assessments of the business or political environment that were never intended for public dissemination. Not surprisingly, some hackers have realized that law firms serve as a clearinghouse for much of the data they seek — receiving, processing, analyzing, storing, and distributing such information.

Importantly, while law firms are now squarely on hackers' radar, lawyers have been slow in some cases to appreciate the significance of the threat posed by cybercrime to their practices. While most every major firm in the United States has implemented some form of information security policy, experts estimate that upwards of 80 major law firms were nevertheless successfully hacked in the past year alone. *See*, Michael A. Riley and Sophia Pearson, "China-Based Hackers Target Law Firms to Get Secret Deal Data," *Bloomberg* (Jan. 31, 2012). And in more than five out of every six breaches, the infiltration remained undetected for weeks at a time. *See*, "2012 Data Breach Investigations Report," Verizon Communications, at 3 (2012) (http://bit.ly/GFfpdk). Because breaches tend to be under-reported, these figures are likely just the tip of the iceberg. Yet law firms remain largely under-prepared to meet the challenges for which they are increasingly being targeted.

Contributing Factors

Many factors contribute to this delayed reaction by some, including a perception that cyber security measures can be unduly expensive and may interfere with the ability to serve clients. Such concerns are regrettable, given that more than 97% of all breaches in the past year could have been averted through simple or intermediate

Karl Nelson is co-partner-in-charge of Gibson, Dunn & Crutcher LLP's Dallas office, and a founding member of the firm's Information Technology and Data Privacy Practice Group. He is also a member of the firm's Labor and Employment, Employee Benefits, Executive Compensation, and Class Action Litigation Practice Groups. **Michael D. Y. Sukenik** is an associate in the same office, and focuses his practice on complex litigation, antitrust and trade regulation, and data privacy.

security controls. *Id*. But perhaps most responsible for the slow response by some firms is a misplaced belief that cyber theft affects businesses, not lawyers.

Compounding these dangers is the emergence of the mobile practice of law and a drastic shift in the manner in which law firms and lawyers ply their trade. Through the Internet, attorneys can access files from their homes, on the road, and across the world. This evolution from relatively closed and protected local networks to Internet-based access, wireless connectivity, and cloud computing naturally exposes information to increased opportunity for interception. And with the rapid adoption by lawyers of smartphones and tablets for business communications, information security staffs must now contend with an exponentially greater number of both devices and potential access points to a law firm's network.

At the same time, hackers have grown continually more sophisticated in their exploits. In addition to simply capitalizing on increased network vulnerabilities, cybercriminals have grown adept at socially engineered exploits such as "spear phishing." This entails sending specifically tailored spoof e-mails to company employees that closely mimic, and appear to be a genuine e-mail from, a trusted source. The e-mail typically encourages a recipient to click on a seemingly legitimate attachment or link, but doing so covertly introduces malware into the network, which then provides the hacker access and creates a pathway for the installation of any number of other forms of malicious programs. These new tricks of the hacking trade reflect a contemporary understanding that the brute force of superior software and expert programming is not always necessary to gain the information they seek. Rather, the misplaced trust of even just one legitimate user may be enough.

'Hacktivists'

Likewise, hackers and their motivations have evolved. Traditionally, cybercrime was committed by individuals or loosely organized criminal groups, motivated primarily by personal pecuniary gain. Even today, criminal groups account for the overwhelming majority of all data breaches and for one-third of data breaches targeting larger organizations. *Id*. at 20. But this segment of hackers is only part of the story. More threatening to law firms, perhaps, is the growth in activist and state-sponsored cybercrime in recent years. The same qualities that make the Internet such a potent tool for informal communication and social change allow hackers to easily and anonymously share information and combine efforts to pursue illegitimate goals.

Those interactions have helped fuel a broadening of hacker motivations and targets beyond purely financially driven pursuits, as illustrated by the rise of "hacktivists." These hackers are motivated by the pursuit of notoriety, by animus toward their targets, and by the goal of furthering political or social change by embarrassing and shaming businesses through dissemination of internal information. Significantly, approximately one out of every four breaches targeting large business organizations is now motivated by disagreement or protest, and approximately one out of every five attacks upon large organizations is now coordinated by activist collectives. *Id*. at 19-20. The most famous of these is the aptly named Anonymous, which has become synonymous with large-scale and highly publicized data breaches.

In the past, hacktivists were known for website defacements and coordinated denial-of-service attacks; acts that were injurious, but not intolerably destructive. But today, their arsenal is more sophisticated and has expanded to include data breach and data theft. Given the sensitive information handled by law firms — and the unfortunate fact that their data security efforts may lag behind those of the clients whose information they regularly handle — they are a natural target for hacktivist attention.

Advanced Persistent Threats

Another emerging threat for law firms are so-called "advanced persistent threats," such as those posed by state-sponsored cybercrime. While government involvement in corporate espionage is not new, a number of developing nations have recognized the opportunities presented by the Internet to use hacking as a tool for socio-economic advancement. In particular, much attention has recently focused on activities seemingly linked to state-sponsored groups associated with China. Accordingly, firms representing clients transacting business in China or whose activities may affect the interests of China or other countries with links to state-sponsored hacking must use extra caution. One former Department of Homeland Security official referenced the FBI's warning that his law firm would be targeted if it represented companies in prominent business dealings or litigation with Chinese state-owned or affiliated enterprises. Matthew Huisman, "Online Attacks," *National Law Journal*, at 1-2 (Apr. 23, 2012) (http://bit.ly/NUDDT7). While China is certainly not the only country with seeming links to corporate espionage, hacking campaigns with a Chinese connection are increasingly prevalent and only likely to escalate with China's ongoing integration into international commerce and law firms' expanding involvement in the China market.

Legal and Ethical Duties Regarding Data Protection

Most law firms place a high priority on protecting and enhancing their reputations. And few events are more damaging to a lawyer's or a law firm's reputation than the loss of trust by a client. Whether the injury occurred unwittingly is unlikely to matter where the fact of injury is clear. And if doubts about data security begin to restrict the free flow of information between clients and their counsel, the entire legal profession may suffer. Apart from the specter of reputational and relationship harm, however, law firms face an array of more formal obligations with respect to the protection of their clients' information.

First, all but a handful of states have enacted security breach notification laws. These statutes mandate that all commercial enterprises that possess or process personal information promptly notify any affected parties of a breach of data security. Many of these statutes further require the organization to report the breach to a state's attorney

general. Penalties for failure to provide the required notice vary among the states — ranging from fines to potential civil actions. To the extent a firm handles personal information regarding its clients, it is likely to be subject to such provisions if that data is exposed through a network breach.

While the notification laws focus on an entity's response to a breach, law firms must also consider their obligations to address prospective security risks. Upwards of 10 states have enacted laws requiring the implementation of measures to safeguard personal information; in some instances, legal compliance demands encryption of all files containing any personal information that may be stored on portable devices, or may travel wirelessly or across public networks. *See*, 201 Mass. Code Regs. 17.04 (2010).

Firms must also keep in mind indirect obligations such as those that may arise under the Securities and Exchange Commission's (SEC) recently issued guidance on reporting security issues. The new guidance recommends disclosure by companies subject to SEC regulation of certain "risk factors," such as known or threatened cyber incidents or aspects of a company's operations that may pose a material cyber security risk. The disclosure recommendations do not distinguish between a direct breach of a company's systems and compromise of data held by third parties acting on behalf of a company, such as where the company "outsources" legal functions "that have material cyber security risks." Securities & Exchange Commission, Division of Corporation Finance, "CF Disclosure Guidance: Topic No. 2 — Cybersecurity" (Oct. 13, 2011) (http://1.usa.gov/ppKxqE). Thus, a law firm's breach involving information of a publicly traded client — or even a failure to preemptively secure such information — could potentially implicate that client's disclosure obligations.

Lawyers and their firms must also be conscious of their special ethical obligations to protect client information. Specifically, under ABA Model Rules 1.1 and 1.6, lawyers possess an ethical obligation to safeguard a client's privileged information by taking reasonable precautions against inadvertent or unauthorized disclosure. Given the rise of computer security issues, several state bars have issued advisory opinions emphasizing that attorneys must take "reasonable and competent steps to assure that the client's electronic information" is properly protected. State Bar of Arizona Opinion No. 05-04, at 1 (July 2005) (http://bit.ly/IcBp4W); *see also*, New Jersey Committee on Professional Ethics Opinion 701 (April 24, 2006) (http://bit.ly/HnsiNV); Nevada Standing Committee on Ethics and Professional Responsibility Formal Opinion 33 (Feb. 9, 2006) (http://bit.ly/MKKkYE); Virginia Standing Committee on Legal Ethics Opinion 1818 (Sept. 3, 2005). But the reasonableness of such measures is not necessarily judged by what a lawyer might view as sufficient. Rather, lawyers must "recognize their own competence limitations regarding security measures and take the necessary time and energy to become competent" or must consult experts in the field. State Bar of Arizona Opinion No. 09-04, at 2 (Dec. 2009) (http://bit.ly/86gZg9).

Echoing this approach — and perhaps recognizing the inertial resistance to change that sometimes plagues lawyers — the ABA has proposed a similar amendment to the existing Model Rule 1.6, which would emphasize the ethical obligation to protect confidential information from "inadvertent disclosure [ ] or unauthorized access." ABA Commission on Ethics 20/20 Initial Draft Proposals — Technology and Confidentiality, at 6 (May 2, 2011) (http://bit.ly/OvwoEU). Given the rise in cyber security attacks targeting law firms and lawyers, these state bar advisory opinions and the ABA's proposal make clear that law firms can no longer treat the security of electronic information as a secondary concern.

Conclusion

The mounting danger of cyber attacks, combined with the convergence of several trends that place law firms at particular risk, provides a timely reminder that cyber security in the practice of law can no longer be an afterthought. Law firms offer one-stop shopping for hackers: a single, centralized focal point with access to sensitive information for multiple clients in the most salient fields of business. And hackers, like water, seep away from hard surfaces to more permeable ones. While firms may present an attractive target to the extent they lag behind other businesses in protecting against cyber attacks, they can often greatly reduce the chances of becoming a victim by implementing basic security measures. While "best practices" are constantly evolving and beyond the limited scope of this article, the greatest tool in the battle for data security is awareness. Law firm personnel who have solid understandings of the risk of potential hacking activity are more likely to be vigilant for its signs. And unlike the crew of the "unsinkable" Titanic, they will be much better equipped to recognize the signs of a cyber attack and to raise the alarm before it's too late.