New Jersey Law Journal

VOL. 207 - NO 6 MONDAY, FEBRUARY 6, 2012 ESTABLISHED 1878

Law Office & Trust Account Management

The Network Security and Privacy Gauntlet

By Kurt W. Krauss and Paul E. Paray

Bradford Bleier, a unit chief in the Cyber Division of the FBI, offered up the obvious in November 2011 at the 19th Annual Review of the Field of National Security Law: "Law firms have tremendous concentrations of really critical private information" and breaking into a firm's network "is a really optimal way to obtain economic and personal security information."

Yet, despite this attraction, law-firm data breaches rarely hit the papers. Thankfully for law firms, it seems that low-hanging fruit with larger stores of data have taken the attention of criminals — leaving only sporadic reported incidents such as the cyber attacks against Gipson Hoffman & Pancione in Los Angeles after the law firm represented software maker CYBERsitter, LLC, in a $2.2 billion software piracy action filed against the People's Republic of China and seven major computer manufacturers. It may be that law firms are less focused on data security than financial institutions and health-care organizations, which routinely report breaches, and, as a result, law-firm breaches may go undetected. Those breaches that are discovered, however, may not require disclosure if the exposed information is not the type that triggers notification obligations under the statutes.

New Jersey's data breach notification law, N.J.S.A. 56:8-161-166, requires law firms to notify only when the breach involves Social Security numbers, driver's license numbers or financial account information that includes a security code — the sort of information many law firms never need to obtain in the first place. Moreover, even if a breach required notification, a managing partner's security concerns might not hit fever pitch given that suits arising out of a breach rarely survive motion practice. For example, see *Reilly v. Ceridian Corp.*, 2011 U.S. App. Lexis 24561 (3d Cir., Dec. 12, 2011), finding that "allegations of an increased risk of identity theft resulting from a security breach" are insufficient standing alone to secure Article III standing (affirming dismissal of claims brought by former employees of a New Jersey law firm after the firm's payroll processor was breached). Even if a lawsuit stemming from a data breach may ultimately be dismissed, most firms would still prefer to avoid the reputational damage that easily could flow from a publicly disclosed data-breach incident.

Many New Jersey firms would benefit from evaluating their network security and privacy processes and protocols. Procedures that apply to protecting personal information would equally apply to protecting other sensitive information — from strategy for an upcoming trial to plans for a client's patent prosecution.

IT Due Diligence for Law Firms

Safeguarding client data already is deeply rooted as an ethical requirement. Under New Jersey's Rules of Professional Conduct, RPC 1.6(a), a lawyer generally "shall not reveal information relating to representation of a client unless the client consents after consultation …." This firmly entrenched confidentiality obligation couples with other ethical duties to create an internal as well as external digital risk framework:

- RPC 1.1(a): "A lawyer shall not [h]andle or neglect a matter entrusted to the lawyer in such manner that the lawyer's conduct constitutes gross negligence."
- RPC 1.9(c)(2): "A lawyer who has

Krauss is a partner and Paray is of counsel at the Florham Park office of Wilson, Elser, Moskowitz, Edelman & Dicker LLP. Krauss has extensive litigation experience handling complex cases in the area of commercial and business disputes. Paray is a commercial litigator who also counsels clients on managing technology risk.

Reprinted with permission from the FEBRUARY 6, 2012 edition of *New Jersey Law Journal*. © 2012 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited.

formerly represented a client in a matter … shall not thereafter … reveal information relating to the representation ….”

- RPC 5.3: “… every lawyer, law firm or organization authorized by the Court Rules to practice law in this jurisdiction shall adopt and maintain reasonable efforts to ensure that the conduct of non-lawyers retained or employed by the lawyer, law firm or organization is compatible with the professional obligation of the lawyer.”

Understanding that “the problems of unauthorized access to electronic platforms and media (i.e., the problems posed by ‘hackers’) are matters of common knowledge,” the New Jersey Advisory Committee on Professional Ethics built on this existing ethical framework in its Opinion 701, 184 N.J.L.J. 171 (April 10, 2006). Specifically, in approving a firm’s document digitization efforts, the committee had the occasion to opine on an attorney’s obligation to safeguard client data from a data breach or loss. The committee first acknowledged that the “obligation to preserve client confidences … requires that the attorney take reasonable affirmative steps to guard against the risk of inadvertent disclosure.” It also reaffirmed that a lawyer is required to “exercise sound professional judgment on the steps necessary to secure client confidences against foreseeable attempts at unauthorized access.”

Recognizing that what constitutes proper safeguards under the rules “may be informed by the technology reasonably available at the time to secure data against unintentional disclosure,” the committee not-so-subtly imposes an IT due diligence obligation on law firms. As for vendors, the committee did not read the rules “as imposing a *per se* requirement that, where data is available on a secure web server, the server must be subject to the exclusive command and control of the firm through its own employees.” According to the committee, “reasonable care” against unauthorized disclosure is exercised when “(1) the lawyer has entrusted such documents to an outside provider under circumstances in which there is an enforceable obligation to preserve confidentiality and security, and (2) use is made of available technology to guard against reasonably foreseeable attempts to infiltrate the data.” Other states have reached similar conclusions when discussing the acceptable use of IT providers. See, Fla. Bar Op. 06-01 (April 10, 2006); NY Bar Op. 842 (Sept. 10, 2010).

Evaluating the Risks

Although it is too early to tell whether 2012 will see an increase in law firm digital exposures, law firms may benefit from evaluating vendor controls, policies and procedures for acceptable use of social media and reviewing smartphone security.

• *Vendor Engagements*

According to the Ponemon Institute, which conducts independent research on privacy, data protection and information security policy, 29 percent of all breaches are caused by third-party negligence. Thus, with vendors such as copying services and the like being used by law firms, it is a good idea to keep in mind the New Jersey Advisory Committee on Professional Ethics’ requirement that vendor agreements have an “enforceable obligation to preserve confidentiality and security.” A law firm also could consider better evaluating the background of vendors that process or hold its sensitive data. It also pays to find out early if the vendor understands data security issues and has a process in place to safeguard the firm’s sensitive data. The adage “trust but verify” is a useful concept, especially if audit rights are built into the vendor engagement.

It also makes sense to ask vendors for an insurance clause in their contracts, requiring certain minimum insurance coverage, including network security and privacy insurance that covers liability expenses related to a breach incident as well as forensics and notification expenses. On that note, it may also make sense for a firm to evaluate such insurance for itself, given coverage would be triggered even if the data thief was the third-party provider. The underwriting process is also a good independent and cost-free check on a firm’s security and privacy processes.

• *Social Media Policy*

How a law firm addresses social media use can assist in mitigating digital risk exposures. The first two sentences of the New Jersey Supreme Court opinion in *Stengart v. Loving Care Agency, Inc.*, 201 N.J. 300 (2010), nicely underscore the difficulty all firms have in curbing online activities: “In the past twenty years, businesses and private citizens alike have embraced the use of computers, electronic communication devices, the Internet, and e-mail. As those and other forms of technology evolve, the line separating business from personal activities can easily blur.” Unfortunately, this blurring of online social and business activities creates newfound security problems for firms.

As noted in a July 2011 study by the Ponemon Institute, a company’s increase in social media use directly relates to increases in a company’s risk for viruses and malware. Indeed, the study found that more than one-half of the businesses surveyed reported an increase in cyber attacks as a result of employees’ use of social media networks. Further, only 35 percent of firms worldwide had a social media “acceptable use” policy in place, and of those, only 35 percent actually enforced it. Social media “acceptable use” policies are complicated by free speech rights and blurring of the lines between business and social activities. In this context, care must be taken in drafting social media policies to minimize difficulties that may result when enforcement is undertaken. Training concerning the risks associated with social media may also help law firms to reduce risk.

Some law firms may find that having a comprehensive policy that applies to internal as well as external use of social media can go a long way in helping to avoid data breaches. For example, hackers may start out by compromising a perceived trusted relationship, such as a social media connection or family member’s e-mail address, to lure a victim into clicking on an image or website laden with malware. Not surprisingly, criminals often set up false social media profiles to gather the information necessary to launch more targeted attacks.

For now, a good way to combat the threat of cyber attacks based in compromised trusted relationships is to educate employees about these risks. Some firms may decide to put written policies and procedures in place to limit usage and resulting risk. Others may determine that access at work to social media, such as Linkedin, is important to the firm’s reputation and business. Also, many law firms routinely view social media use by opposing parties, as well as by other lawyers and business partners, just as they would analyze other publicly available information about busi-

ness partners and opponents. There is no one-size-fits-all solution to social media issues, but it is worthwhile for a law firm to consider these issues and make informed decisions concerning them.

• *Smartphones*

Most IT managers are well aware of the harm that can result when a laptop is lost or stolen, and as more lawyers use smartphones, the evolving technology presents new challenges. When a smartphone is lost, stolen or accessed without authority, the amount of data that is compromised can be significant. Cyber criminals look for comparatively easy access points, and smartphones may be a weak spot in a firm's information security. A study conducted by market researcher Ovum and the European Association for e-Identity and Security found that half of the organizations surveyed fail to authenticate their employees' mobile devices, among other basic security measures.

One way to enhance smartphone security is to use a strong password (not surprisingly, including a capital letter and number or character increases the strength of passwords) and change it at regular intervals. Training users to delete suspicious e-mail, in the same way it is done on a laptop or work computer, further enhances smartphone security. Evaluation of antivirus protection also may be worthwhile. In addition, using the screen saver feature with a password will lock down a smartphone in the same way laptops are locked down. More advanced security features that may be appropriate, depending on the intended use of the smartphone, include remote wiping applications, encryption and data leak prevention tools.

Reasonable Steps

Theoretically, there is always more that could be done to strengthen a firm's defenses and procedures. No system is bullet-proof, as cyber criminals continually adapt to the ever-changing environment in which they operate. As a result, no firm's information can ever be 100 percent secure. In this context, the reasonable steps that a firm takes to secure information are relevant from both a client relations perspective and an ethical perspective. By committing resources now to evaluate the safeguards currently in place, firms are not only doing the "right thing" but also lessening the likelihood that they will be a party on the wrong side of a civil complaint or ethics grievance. ■