The Soft Underbelly of Corporate America

Law Firm Cybersecurity, Ethics and the Changing Field of Play

By Edwin B. Reeser and Martin J. Foley

Lawyers may be way behind and losing ground at effectively coping with storage, maintenance and use of client confidential data and fulfilling significant ethical obligations regarding data leakage prevention/protection (DLP). Data leakage prevention is a system designed to detect potential data breach/data ex-filtration transmissions and prevent them by monitoring, detecting and blocking sensitive data while *in-use* (endpoint actions), *in-motion* (network traffic), and *at-rest* (data storage).

Would you consider the following to be "secrets" of your clients? The take-over strategy for a public company? A trade secret formula you are litigating? A client's bottom line acquisition terms in negotiations for an office building? Details of an approaching public offering of securities? Of course you would. So would your clients.

Before the widespread use of desktop computers in business and law (less than 30 years), lawyers could secure such secrets in locked filing cabinet drawers, in a locked office, in a building that had security guards and sleep peacefully knowing we had complied with our ethical duties. Hypersensitive information, say an actual government classified document or a patentable idea, typically required further steps similarly based on physical, mechanical steps such as putting documents in a locked vault inside a secured facility. Before the widespread use of the Internet in business and law (less than 20 years), what was inside computers was similarly secured through physical access restriction.

Today almost all "secret/confidential" information is stored somewhere on the law firm's computer systems, and for some firms in the "cloud." That information may be password protected; it may be encrypted; it may be user access limited; but it can still be accessible and transportable through cyberspace.

California Rule of Professional Conduct 3-100 addresses our ethical obligations for handling confidential client information. That rule mandates that "(A) A member shall not reveal information protected from disclosure by Business and Professions

Code section 6068, subdivision (e)(1) without the informed consent of the client, or as provided in paragraph (B) of this rule [which deals with the prevention of criminal acts]." But Section 6068 is a potential nightmare when considered in relation to a client's computer-stored information in your law firm's possession. The section provides: "It is the duty of an attorney to do all of the following:

(e)(1) To maintain inviolate the confidence, *and at every peril to himself or herself to preserve the secrets*, of his or her client." (Emphasis added.)

Moreover, a member's duty to preserve the confidentiality of client information involves public policies of paramount importance. *In Re Jordan*, 12 Cal. 3d 575, 580 (1974). Preserving the confidentiality of client information contributes to the trust that is the hallmark of the client-lawyer relationship. Thus, paragraph (A) of Rule 3-100 recognizes a fundamental principle in the client-lawyer relationship, that, in the absence of the client's informed consent, a member must not reveal information relating to the representation. *See, e.g.*, *Commercial Standard Title Co. v. Superior Court*, 92 Cal. App. 3d 934, 945 (1979).

Do you imagine that the standard of care we will be held to for measuring compliance with Rule 3-100 and Section 6068 is the "locked drawer" paradigm of the 1970s, or the best available technological solutions of the second decade of the 21st century? What will clients expect and require, as a condition to the law firm being awarded a work assignment? Will clients increasingly require proof of the capability of the firm's system to protect confidentiality of client data before it is entrusted to the law firm? The answers are self-evident.

The threat of data or information breach comes in two generic forms: *intrusion* (threats from outside) and *extrusion* (threats from inside the firm).

The vast majority of current law firm cybersecurity efforts tend to focus on *intrusion threats*. Solutions to this have focused on firewalls, randomly generated passwords, limited user access, password protected files, encrypted files, intrusion detection systems (IDS), intrusion prevention systems (IPS), etc.

We are all familiar with hackers. (On Nov. 1, 2009, the FBI issued an advisory warning to law firms that they were specifically being targeted by hackers.) They come with many levels of expertise. For this article we generally rank hackers at

A, B and C skill and resource levels. A-level hacker superstars target high value, top security locations such as the Department of Defense, Department of Energy, Atomic Energy Commission and the like. B-level hackers aim at large or technologically advanced corporations for industrial espionage purposes — your General Electrics, Boeings, and Adobes. Law firms are the daily bread for mere C-level hackers. Indeed, in 2011 the U.S. government labeled New York City's 200 largest law firms "the soft underbelly" of hundreds of corporate clients. At an ABA Techshow session on data security for lawyers, presenters Sharon Nelson and Ben Schorr warned that even midsize, boutique and solo firms are at risk, and untrained lawyers and office personnel are often the No. 1 chink in a law firm's defense.

This simple ranking does not account for the army of criminals who beat ATM machines, steal identities and infiltrate home computers. Consider that many sovereign nations maintain talent backed by substantial budgets, hardware and other support at all three levels, to pursue their "interests." How many nations would be interested in an international transaction impacting control of a major natural resource or technology? Would they want to take a look? Do you think that they aren't? When law firms are announced as counsel for the various parties in the deal, which system is likely to be easier to crack to find what they want — the client's or the law firm's?

Intrusion threats are only half the battle. To be ethically compliant, we must increase DLP efforts on *extrusions* — data leaking from inside firms to outside parties. Data *extrusions* occur in numerous ways, inadvertently — by accident or negligence, by poor controls, by industrial espionage, or by criminal acts. "Lawyer Convicted in Insider Trading Scheme Disbarred," Blog of the Legal Times of Washington, D.C. (Nov. 21, 2013).

You may know and trust your own personnel, but do you have controls? What prevents a staff person or attorney from being paid or coerced into plugging a thumb drive into the system to load a program or masquerade as an authorized user, enabling unrestricted access? What prevents in real time an electronic transmission, or download to a portable storage device for physical removal of the confidential information … in seconds?

When third parties are introduced, such as outside vendors in e-discovery projects, another data loss risk emerges. How do you perform due diligence about temporary workers hired by third-party vendors?

The reality and unacceptable consequences to lawyers of data *extrusion* is exemplified by the current Apple/Samsung litigation which (secondary to that complex case) involves potential sanctions for leakage of trade secret and protective order protected data. *Apple Inc. v. Samsung Electronics Co. Ltd. et al.*, 5:11-cv-01846 (N.D. Cal.).

What can we do about these ethical and practical challenges? There are four basic approaches law firms are utilizing presently.

1. **Invest in a secure computer network system**. This approach has significant control benefits. A firm can craft its own cybersecurity system tailored to its particular needs. Unfortunately, minimum estimates for sophisticated systems start at around $25 million. Then add on-going maintenance and update costs of approximately $2-3 million per year. Capital outlays of this magnitude are available only to a small segment of law firms. Less robust systems can be installed, but even these likely require at least a $10 million investment.
2. **Establish an adequate internal computing system with a separate e-discovery/special document handling function under direct control.** Some firms have set up their own litigation/transaction support and document handling function as part of their law practice. This approach certainly is workable; yet costs may be a significant barrier to entry for the majority of firms and management talent shortfalls present additional challenges.
3. **Partner with corporate clients in appropriate cases to establish a document management/litigation support function within the client's organization.** With large companies and large cases, teams can be established using outside and in-house counsel and staff to do a creditable job protecting and utilizing data and documents for litigations and transactions.
4. **Coordinate with the client to hire and direct third-party vendors specialized in DLP.** This approach is presently the most broadly applicable

> solution and fits almost any size firm and client problem. It provides both flexibility and scalability. Lawyers do their job providing legal and strategic analysis and guidance to identify case issues and solutions, maintain privileges, and prepare the matter for trial or closing, as the case may be. The third-party vendor does what it specializes in: providing DLP against threats of *intrusion* and *extrusion*, data management and document organization and handling and, if desired, litigation/transaction support functions as well. Each entity, legal and data security, does what it does best. The start-up DLP cost (basic infrastructure, facilities and equipment) can be spread over numerous clients and firms because the fixed facilities and advanced systems costs are borne by the data security company. The flexibility of this solution is extensive. Think of the data security facility as a hotel. If you wanted to go to Las Vegas, you wouldn't build a resort hotel for yourself; you'd rent a room. If you were a convention, you might take over many facilities and rooms for the event. Similarly, if the data security company is properly organized, your small case may only need to pay for a room in the hotel for a night or a week. If you have a larger case, you may want a suite and conference room. With this model, you can scale up to the largest matters. And you can select the appropriate levels of security as the matter, or selected parts of the matter, justifies.

There are several DLP entities with capabilities to fit your clients' cybersecurity requirements. Check the Internet using keywords: cybersecurity, data leakage prevention or protection, for a good start.

Consider a cybersecurity audit testing of the DLP security of your firm's systems. This audit is easily accomplished using outside vendors, staging various cyber "attacks" to evaluate the adequacy of your system security.

Compliance with your ethical obligations requires that you examine DLP issues and apply solutions that best fit you and your firm's circumstances.

But client DLP isn't the only obligation to be considered. What about issues of privacy? Will DLP systems be programmed not only for protecting client confidences, but also for spying on lawyers and staff for other purposes? Is it not one thing to protect the client's formula for a cancer drug, and quite another to

have your email to a partner auto-flagged because you referred to the managing partner as a "dork"? At what price and using what balancing criteria can we resolve this, and many other conflicts, in protecting rights, duties and expectations of privacy within the firm, as we deal with protecting client information? It is not adequate to consider these issues in a piecemeal fashion. We need to think about them as elements of an integrated, comprehensive DLP/cybersecurity plan for the benefit of ourselves and our clients.

Edwin B. Reeser is a business lawyer in Pasadena specializing in structuring, negotiating and documenting complex real estate and business transactions for international and domestic corporations and individuals. He has served on the executive committees and as an office managing partner of firms ranging from 25 to over 800 lawyers in size.

Martin J. Foley practiced in BigLaw for 37 years. He served on ethics committees for 15 years, became head of West Coast ethics, and then was nationwide General Counsel for an AmLaw Top 50 firm for five years. He has held US government security clearances and worked on computer systems since 1967. He currently practices trial law in Los Angeles, emphasizing employment counseling, high tech and IP protection.

The authors wish to thank Jim Ramsey (jramsey@epiqsystems.com) and the Epiq Systems, Inc. cybersecurity team for invaluable technical assistance in preparing this article.