

THE **Scitech** LAWYER

VOLUME 4, ISSUE 3 | WINTER 2008 | SECTION OF SCIENCE & TECHNOLOGY LAW | AMERICAN BAR ASSOCIATION

ROBOTS **THE HUMAN BRAIN** AND THE LAW

IN THIS ISSUE



Institutional Review Boards: The Debate Continues
By Eric Y. Drogin and Daniel A. Bronstein4



Harmonizing Health Care IT Standards
By Alan McGrath8



Food Law: What's in Store
By Melissa Ince20

MELISSA INCE AND STEPHEN M. GOODMAN, ISSUE EDITORS

Are We WORTHY?

Is Law Firm
Electronic
Security
Adequate to
Protect Client
Secrets?

By John F. Emerson



As law firms become accustomed to handling more and more electronically stored information (ESI), many are discovering, if their clients have not already done so, that the security of their document husbandry is sometimes light years behind that of their clients. Although many of the largest firms have developed highly sophisticated (and expensive) methods of ensuring the safety of confidential client data, other firms could stand to take a hard look at some easy and cost-effective means of tightening things up.

A Little History

Many lawyers will recall the days of stand alone desktop computers, unconnected to anything except the electri-

cal outlet. Some will even hark back to the trustworthy and sturdy IBM Selectric or even to the more aesthetically pleasing Royal Standard upright. Although networked computer systems eventually replaced these old standbys in the law office environment, law firms did not take to the electronic exchange of information quickly or enthusiastically—and this reluctance still affects how law firms manage and prioritize electronic information security.

Firms did eventually bow to client demands, and proceeded to implement the electronic communication systems that the clients themselves relied on. In the 1980s, cutting-edge law firms took the first step—using a system of modems for confidential and other communications. The firm and client sent each other messages by way of a central service such as AT&T, which ensured that only the designated recipient could receive the messages. Soon after, law firms began instituting local area networks (LANs) for internal e-mail systems. The use of LANs became even more popular when research companies such as CCH discovered they could sell to firms CDs of data that could be loaded onto the local LANs and made available to attorneys through the internal network. Eventually, firms were forced to join clients and the rest of the world out on the World Wide Web.

In the past 15 years, the proliferation of communication-facilitating applications has been blinding. Security, however, particularly as used by law firms, has followed at a more sedate pace. Businesses have been far ahead of law firms in terms of ensuring the security of electronic communications, and continue to be so. And so the question is, how can business trust the secrets it has so closely guarded to the shelter of law firm security?

What Can Go Wrong/ Cautionary Tales

The most serious dangers seem to be those that are posed by persons obtaining data “in the flesh” and not by motivated hackers decrypting secured

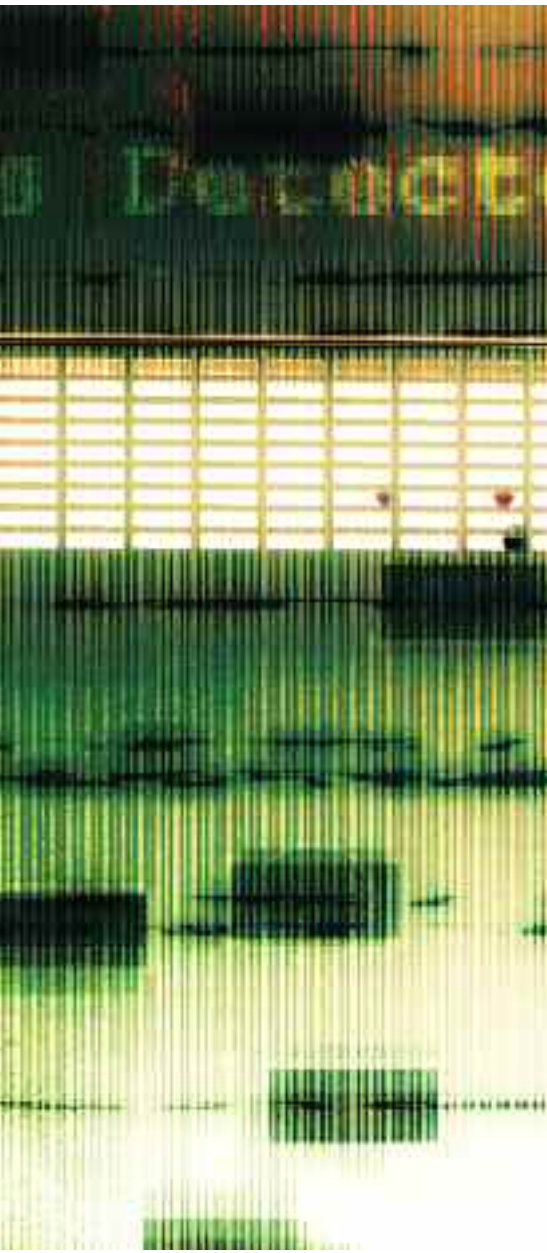
messages or breaking into a firm’s systems. The most significant source of outside access is the third-party vendor. The director of global technology for one of the largest law firms in the United States (hereinafter “Mr. Digital”) stresses the importance of careful screening: In 2002, a 19-year-old college student employed by one such vendor was charged with stealing encryption technology from DirecTV while reviewing DirecTV’s documents on behalf of counsel. The highly confidential information, which represented two years of research and development and a \$25 million investment, surfaced on numerous websites. Although better screening might not have stopped this rogue employee, the story illustrates the potential danger.

A less dramatic anecdote illustrates a more common situation. The IT department of a firm, against a deadline to install new patches on a large number of individual desktops, retained contract technicians to assist. One such technician went office to office introducing himself as working with IT, and asked each attorney to log on for him and then let him have access to the computer for a period of time. Out of the 19 offices he visited, only one person questioned him and called IT to verify the legitimacy of his purpose, and that person was not an attorney. Though the technician in that case was legitimate, such access could have led to disastrous results in the hands of another.

Physically misplacing devices with secured data is also an issue. Erik Petersen of SecureWorks, a managed information security services provider based in Atlanta, recalls working with a major hospital system that had recently replaced some of its desktop computers. The company received a call from an individual who had purchased one or more of these computers on eBay, who discovered that the hard drives contained an enormous amount of ESI related to the hospital system’s internal operations.

Corporate Practices

Consultants who work with major



corporations say business succeeds where law firms may fail for a number of reasons. Probably the greatest factor is simply economies of scale. Consider that the largest law firm in the United States, Baker McKenzie, boasts 3,246 lawyers. According to a recent survey, Wal-Mart, the world's largest employer, has 1.8 million employees; the 500th largest employer in the world employs 21,175.

The revenue generated by these businesses gives them the resources to invest in the technology and the human resources to ensure a greater level of security than all but a very few law firms. A common business hierarchy includes both a chief information officer (CIO), whose sole duties are to maintain information systems, and a chief security officer, whose duties include securing those systems. These positions both report to the chief executive officer (CEO). For these businesses, the importance of staying current on state-of-the-art technology, as well as on security, is manifest.

The way that information technology is addressed in the organizational hierarchy of the law firm is substantially different. The traditional law firm hierarchy has the IT manager reporting to a chief operating officer (COO) who is either an attorney or reports to an attorney. This reflects the typical law firm management view that such technology is just an expense. Chad Todd, chief technical officer for Training Concepts, in Columbia, South Carolina, argues that the positions of CIO and CSO are critical to the success of an IT program, because those officers understand the value of the technology and its security, and report directly to the CEO. Many law firm IT managers are reluctant to press firm management for the funds necessary to maintain adequate security, according

to Mr. Digital. Erik Petersen of SecureWorks agrees: "Mr. [Law Firm] IT guy is harried and overworked. When something goes wrong, management usually fires the IT guy but the problem is usually management's failure to adequately fund and staff."

Another significant difference between corporate IT security and that of law firms is that corporate employees are used to receiving directives and following them, whereas the "end users" at law firms are lawyers who are often reluctant to take instruction from others. Petersen points out that law firms, like physician groups, are "organizationally flat." At a law firm, there is a great deal of power distributed horizontally, rather than vertically, so there are many end users who have the authority to say no to security measures they perceive to be inconvenient or even painful. Mr. Digital agreed that one of the biggest problems for law firm security is the sole practitioner spirit of many lawyers, even in some larger firms.

An example of sophisticated corporate IT security is Blue Cross Blue Shield of South Carolina (Blue Cross), which has 11,000 employees in multiple divisions. A corporate information security council, composed of representatives of each division, legal, management, human resources, physical security, and audit and compliance personnel ensures that Blue Cross meets or exceeds the demands of each of the many audits the company as a whole undergoes each year. Council Chair Jim Daley notes that security measures vary depending on the necessity and efficiency of such measures in each of the distinct divisions. For example, what is practical in the context of their highly secure processing facilities for contracts with the Department of Defense—such as palm-print recognition—may not be practical for use in communications with insureds enrolled under the individual and group health insurance services.

To deal with the third-party vendor security issue, Blue Cross uses a complex system of temporary passwords, and a form of two-factor authentica-

tion when access to the system is granted from a remote location. The user must carry a token or fob, which is about the size of a car's keyless entry device. The token has no buttons but displays a six digit code that is generated through an algorithm, both on the token and on the server. The token displays a new code every 60 seconds. The code generated is unique to the user and is recognized by the network until it expires. If the user fails to log on with the proper passwords and the six-digit code within the prescribed time, the password times out and the user must input the next code generated. With respect to the information security of law firms that Blue Cross retains, Blue Cross's recourse is simply legal action against any firm that suffers a breach of security causing harm to the company.

A senior IT manager at a major utility company, who did not wish to be identified, but who also does IT consulting for law firms (hereinafter "Mr. Terabyte"), said that his company also has many levels of security. His employer operates, among other things, nuclear power plants, which requires the company to comply with in-depth security audits carried out by the U.S. Department of Defense, the Federal Regulatory Commission, the Department of Energy, and the Nuclear Regulatory Commission, among others. Without being overdramatic, Mr. Terabyte said that if you do not have the adequate passwords and clearance to get onto the site of a nuclear power plant, "You will get shot. Literally."

Like Blue Cross, the utility company uses two-factor authentication to access certain systems, but also requires a series of passwords to access any specific database. In addition, company laptops are secured with a power-on password, and an additional password is required to access the network. All data on every laptop hard drive are encrypted, and such data can be tagged, allowing security personnel to track any access or use. Mr. Terabyte said that, in his universe, the only person who could breach the security for

John F. Emerson is special counsel with Nexsen Pruet Adams Kleemeier LLC, with offices in South Carolina and North Carolina. He is a certified specialist in employment and labor law, advising employers on all aspects of human resources management and compliance. He can be reached at jemerson@nexsenpruet.com.



improper purposes is an employee with a high security clearance, and such a person would leave a clear trail.

Mr. Terabyte noted that his company carries out security audits of the law firms they retain, depending on the sensitivity of the issues. In many cases, the company will send a team to perform an on-site audit of the law firm's IT security. Companies of this size want to look behind a law firm's assertions of security, Erik Petersen says, with a note of amusement in his voice. "IT professionals have to do more than say they know their systems are secure; they have to be able to say how they know what they know. That is, engage in a little epistemology."

Mr. Terabyte commented that, in his experience, law firms are behind on IT security: "Most law firms are operated by older men, who didn't grow up in the computer age. They don't understand security issues as well as the younger lawyers, who get it." While these lawyers are interested in technology to make their systems to work faster, synchronizing their PDAs, and improving their secretaries' efficiency, they are less interested in investing in security because they can't see the tangible results. Many don't want to be bothered with even setting passwords on their PDAs, which, he said, are "easy to bust." But if PDAs aren't password-protected and data-encrypted, "your privileged information on your desktop, your email, and your PDA" is exposed.

One Large Firm's Practice

The largest law firms have the resources to retain highly sophisticated staff and to purchase the best and most current technology. In these firms, the bureaucratic control over the individual lawyers is also generally much more effective, and operated more like a corporation.

At Mr. Digital's firm, for instance, absolutely no data get synchronized onto any laptop computer or onto the hard drive of any desktop. In fact, no attorney uses a laptop within the confines of the office; laptops are allowed for remote access only. The firm retains

all of its branch offices' ESI on redundant servers in automated data centers in different locations, so if a computer crashes, no data are lost. And if a laptop is lost or stolen, there is no network data contained therein. Another advantage is that a lost or crashed computer does not hamper an attorney's work. PDAs are required to be locked with a password, and, if one is lost, IT can immediately wipe its contents so that no confidential email or other data are disclosed. In addition, lawyers are required to use two-factor authentication when dialing in to the system from a remote location, and all static passwords are changed every 90 days. Finally, the firm does not use third-party vendors to process or filter its email.

Other technology employed by larger firms includes the use of an access card that, when inserted into a laptop, encrypts the laptop's contents, preventing the content from being accessed by anyone without the card. Third-party vendors must also be carefully scrutinized, says Kevin Jacobs, of DTI Global. These vendors are often used by lawyers attempting to gather and process many thousands of pages of electronic documents, or recover deleted items. Careful screening is critical, he said.

Advice for Everyone Else

For those firms with fewer resources, the experts suggest a variety of steps that can shore up anyone's security. While firms may not be able to justify the expense of palm-print security or two-factor authentication, IT security and maintenance must be given a higher priority.

- To the extent possible, a budget sufficient for IT teams to be adequately staffed with qualified professionals must be provided.
- The budget should also allow for appropriate technology and the constant search for software updates and patches.
- The access of outside consultants must be limited and must

be revoked at appropriate times, because such consultants are the most capable of causing harm without leaving a trail.

- Potential security breaches associated with such problems as unsecured PDAs, unencrypted data, and laptops with no passwords or encryption should be addressed. Of critical concern to many of those interviewed was the physical security of each law firm. Wherever data are on display on a computer that hasn't timed out, or strangers are who can access less public areas of the firm, there is a security risk.

All of those interviewed agreed that lawyers must become acclimated to a culture of securing their own devices and understanding the security risks that their actions or inactions may cause.

Despite the technological issues, the consensus is that the people-factor poses the greatest risk. Careful screening of new, contract, and temporary employees is a must. When hiring outside vendors that may have access to sensitive information, lawyers should involve their own IT professionals to ensure that these vendors are reputable and have adequate security systems themselves; no law firm wants its clients' secrets posted on the Internet. ♦