Law Firm Inc.
IDEAS & INNOVATIONS FOR FIRM MANAGEMENT NOVEMBER/DECEMBER 2006
ALM

Operations

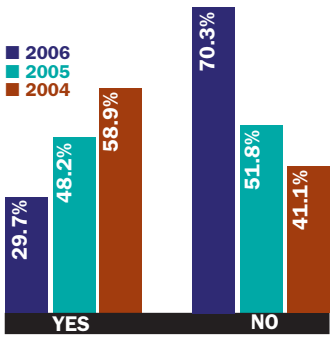
PLANNING & EXECUTION

CLIENT SATISFACTION

They're satisfied, they're really satisfied — and that's music to Am Law 200 firms that have been hiring more client-liaison managers in recent years. That's because fewer chief legal officers are complaining about the responsiveness of the law firms they hire, according to a recent survey by Altman Weil and LexisNexis Martindale-Hubbell. Between 2000 and 2005, "lack of responsiveness" was the primary reason cited by 50 to 60 percent of respondents who were thinking of firing a law firm. This year, that number dropped to 30 percent. But it's not all good news: The top reason cited for firing a firm was bad legal work.

— James Erik Abels

HAVE YOU FIRED OR ARE YOU CONSIDERING FIRING ONE OF YOUR LAW FIRMS THIS YEAR?



A Delicate Balance

Securing client data in a client friendly way

By Judi Flournoy

The security of client data is a paramount concern for every law firm IT executive. But as you look for ways to batten down the hatches, it's important to consider how security measures may impact the overriding goal of any firm — providing quality client service. Focusing too squarely on security or client service, without regard to the other, can mean that one of the two will suffer. At Loeb & Loeb in Los Angeles, we designed our systems with this in mind. Indeed, there are many ways to address security issues without hindering client service.

Information has Value

Chief information officers should ask themselves whether they can guarantee the integrity of everyone at their firm. What about people outside of the firm? The truth of the matter is no one can. As a result, the responsibilities of law firm CIOs have expanded beyond managing technology, and now include managing security. Data security in law firms has long surpassed the use of passwords, and it's important to note that the risks are very real. There have been more than 135 data breaches at various businesses

and government agencies, including a law firm, since the beginning of 2006, according to the Privacy Rights Clearinghouse based in San Diego.

Law firm technology has always been focused on enhancing client service and, to the extent possible, doing so in a way that does not impede an attorney's ability to work. CIOs regularly face the challenge of getting attorneys to change their work habits. Simply asking them to routinely change their password, or to password protect their handheld device can be met with resistance. If information has value, then all of our data is at risk. As CIO, my job is part educator, part policy maker, part strategist, and part warrior (with a few carefully chosen battles). Here are some of the security measures that we've put into place to protect our clients, as well as the data related to our employees.

Passwords and Policies

Passwords are the base of any firmwide security program. Every six months, our system prompts users to change their password; if they do not, they are locked out of the system. Many studies indicate that workers assume the company's IT department handles security. Actually, it's the individual users of a firm's network who are handling security on the "front lines" and are the cornerstone to a successful firmwide security program. It is dangerous to assume that everyone at your firm takes security seriously.

Our firm has a computer security policy that is distributed to every person at the firm. If your firm does not have a policy, draft one and make sure that it stipulates how data is handled. And be sure to periodically review it. Should the firm institute significant changes, the employees should be required to sign the updated policy.

What's more, be sure to include information about your firm's security policies in responses to client RFPs, because clients are interested in where their firms stand on these issues and often are curious about what best practices are being used.

Data Integrity

Where does data live? Most law firms use a document management system, but firm documents live in more than one place. They may be on the local drive of a PC, in an e-mail "Sent Items" folder, on a flash drive, and on a home computer. Keep in mind that most places where work product may be found are out of your control. Therefore it's important that your computer security policy addresses data storage.

A policy that covers issues beyond the traditional concepts of threats within your walls, is an approach that your clients will appreciate. For instance, disk encryption and home security requirements, such as encryption on home wireless networks, are two of the measures we've taken this year. We implemented a home security assessment program that includes an evaluation and any necessary upgrade of the existing home setup and installation of up-to-date anti virus and firewall software. These efforts not only protect the firm's assets but also the client. There is nothing more embarrassing then sharing a virus with a client or exposing client data to prying eyes.

Work Product and Privilege

The Patriot Act, the HIPPA Act, and Sarbanes Oxley have all influenced how we and many of our clients handle data. Many of these newer laws and regulations put forward conflicting requirements. On the one hand, firms must maintain the confidentiality of client and personal data; on the other hand, in some situations firms may be required to divulge certain information.

Applying security to your data is the first step and the only way you will be able to respond to a request for information without inadvertently breaching confidentiality. At Loeb & Loeb we use iManage as our document management system, and it's set up so that newly created documents are not secure unless someone specifically applies security, such as making the document private, so that only the author has access. On the network, only personnel who need access to specific information have access to that data — e.g., accounting, payroll, and human resources have permissions to those areas. Our Elite accounting system and ADP, our payroll system, reside on their own servers. Humanic, our human resources database, is a hosted system.

> "As CIO, my job is part educator, part policy maker, part strategist, and part warrior."

Ethical walls are now a critical component in our electronic data environments as the volume of electronic information increases. To ensure that any conflicted attorneys are walled off, we use an Integration Appliance (IntApp), to generate our ethical walls. The process is automated so that when our conflicts department notes a conflict in Elite, it triggers a rule-based action from IntApp that secures client or matter data in FileSurf, our records management system; iManage; and Elite, our accounting system. These security measures are transparent to the users of the network and do not affect their day-to-day activities.

Meeting Challenges

It's a significant hurdle to put sufficient security into place in a way that does not hinder productivity. We use a number of tools, policies, and approaches including two-factor authentication for remote access, using RSA Security's SecurID; Juniper Network's Netscreen for end-to-end security using SSL connections to our remote desktop; e-mail; and accounting systems. This year we set up secure wireless networks in our Los Angeles and New York offices using Cisco Systems' Aironet product to distribute security certificates, which ensures that only authorized personnel can use our wireless network. We also provide guests with a login and password to our guest wireless network, which is segregated using a Virtual Local Area Network.

Instant messaging is another technology that many of our attorneys have come to rely upon to communicate with clients. This year we deployed Microsoft's Live Communication Server to facilitate secure, encrypted instant messaging. Had we not provided secure instant messaging, we would have been forced to restrict its use and thus negatively impact client service.

Additional Tools

- Snort is an open source network intrusion utility. Essentially a packet sniffer, it has rules that perform content pattern matching and detect a variety of attacks and problems such as buffer overflow and stealth port scans; www.snort.org.
- Qualys offers network security audits and vulnerability management. Under our arrangement with Qualys, the company provides a network appliance that continuously tests our network from the inside. We also use QualysGuard, a service that tests our network from the company's public servers and provides us with reports indicating whether a vulnerability has been detected, such as a SQL server missing a security patch; www.qualys.com.
- Nessus is an open source vulnerability scanner and is endorsed by the SANS Institute, the leading organization in computer security training. It has the ability to detect remote flaws on our network, including missing patches; see www.nessus.org and www.sans.org.
- Cisco Content Security and Control provides threat protection and content control at the Internet edge providing comprehensive antivirus, anti-spyware, file blocking, anti-phishing, URL blocking and filtering, and content filtering services.
- Postini is a hosted service that provides spam and virus blocking.

In the end, whether it's data concerning the firm or data about the client, it's our ethical obligation to do all we can to ensure its security. The roles of policy, software, and hardware are clear. They must be balanced in a manner that promotes efficiency, supports teamwork, fosters compliance, provides access to information, and supports working anywhere, anytime. LFI

Judi Flournoy is CIO of Loeb & Loeb in Los Angeles. E-mail: jflournoy@loeb.com.

This article is reprinted with permission from the November/December 2006 edition of LAW FIRM INC. © 2006 ALM Properties, Inc. All rights reserved. Further duplication without permission is prohibited. For information, contact ALM Reprint Department at 800-888-8300 x6111 or visit www.almreprints.com #014-12-06-0001