

Inside			
Finance	22	Client Matters	33
Q&A: Kean Miller	24	Diversity	36
On Management	27	Marketing	38

NETWORK SECURITY

Armed and Dangerous

Don't overlook employees as a potential threat to your firm's network. **By Lorelei Laird**

They're out there and they're armed. They're armed with knowledge of the vulnerabilities of your law firm's IT systems that could bring operations to a grinding halt or expose the firm to liability. They know where confidential information is kept, what data is essential, and they already have access to the network. Who are they? They're your colleagues.

In the end, a firm's IT systems are only as secure as its employees' intentions and actions. Witness that close to 70 percent of network security incidents at Fortune 500 companies are caused by employee actions — 30 percent malicious and another 39 percent inadvertent — according to a 2004 survey by the Ponemon Institute, an Arizona think tank.

When insiders strike, the price can be steep. More than \$69 million in profits was lost by 700 U.S. organizations in 2004 due to unauthorized access, theft, and insider abuse or sabotage, according to a survey conducted jointly by the FBI and Computer Security Institute, an industry trade group. Because of their legal and ethical obligations to clients, law firms may face an even steeper price. "If, for instance, there's a sensitive litigation going on and the documents escape, the loss to the client and perhaps to the firm due to malpractice can be enormous," says Philip Zawa of legal technology consultancy Baker Robbins & Co. in Chicago, "it can be millions."

Law firm managers probably worry most about the security risks posed by a fired employee with a grudge, and for good reason. A disgruntled systems administrator "could decide to erase anything and cause a severe outage," says Zawa. "If they're really devious, they could erase backups too." But even employees leaving on good terms may be tempted to snag confidential client information or proprietary forms. "I'd say it's pretty routine for lawyers who are leaving to take at least a few [documents]," Zawa says.

The good news: There's a wide array of technology available to keep a firm's system secure. The better news: Zawa says that most law firms already have a lot of the tools they need, because security features are almost always incorporated into the software used by firms. For example, document management software and authentication systems generally have a logging feature, which tracks

where users have been on the network and what they've done.

The first step toward better data security could be as simple as enabling that feature, clearing storage space on servers for the logs, and having an IT or human resources employee review them on a regular basis. Logs can get very big very quickly in a large firm, but automated security tools, such as those built into Microsoft server software, can be set to flag only unauthorized access. For

"If they're really devious, they could erase backups too."

authorized access, however, having a person look the logs over is the only way to catch suspicious activities, Zawa says.

Even if a firm doesn't have the resources to have someone routinely review logs, they provide an essential record if someone is suspected of network tampering. Brian Conlon, CIO at Washington, D.C.-based Howrey, says logs are also useful when data is lost accidentally, because a records administrator can review a log to find out who was the last person to use a missing file.

Another smart security move: limiting access to information on a need-to-know basis. George Yorty, operations manager for systems and technology at

Pittsburgh-based Reed Smith, uses the security feature of its document management system, DOCS Open from Toronto's Hummingbird Ltd., to accomplish this. He's able to define access levels for broad groups of users such as "West Coast paralegals," he says, as well as limit access to just the one or two partners working on a particular case.

If a firm needs to review an employee's e-mail, Baker Robbins' Zawa says there are e-discovery programs intended for use in litigation that can be used just as well on an employee's messages. To avoid privacy conflicts, a firm should ensure all employees have signed a policy stating that the firm owns any e-mail sent using its systems. To block inappropriate e-mail, there are business software applications called Acceptable Use Policy software, which are similar to the content filtration software used by schools, but much more advanced and designed for large businesses.

Howrey's Conlon says his firm uses iPrism and ePrism from San Diego-based St. Bernard Software, which uses a physical appliance and software to filter and flag inappropriate e-mail and Internet usage, keep an eye on online activity, and block viruses. A company salesman says large firms can expect to spend \$2,195 for its filtering/watchdog software and \$1,295 to \$50,000 annually for updates, depending on the number of computers protected.

Another package that provides Conlon with a security "extra" is Network Toolset, a network management and monitoring tool from Tulsa-based SolarWinds.net, Inc. It measures and protects virtually every aspect of Howrey's network usage, such as bandwidth, disk space, and processing power, and provides tools to detect and defend against security holes like open TCP/IP ports (Internet access to the network) and find out when others are blocking messages from firm e-mail servers.

But a feature Conlon finds especially useful is the program's ability to flag unusual activity. If, for example, uploads (network-based data sent onto the Internet) by all network users pass a pre-set threshold, the program pages the firm's IT team. Conlon can also set it to watch individual users for any suspicious behavior. "Generally, the profile of someone's network traffic is pretty consistent," he says. "If they go above and beyond . . . we can isolate [the activity] down to a particular device and shut



Howrey's Brian Conlon

"Generally, the profile of someone's network traffic is pretty consistent."

them off." Network Toolset runs from \$145 to \$995, depending on the number of features needed.

Products designed to prevent data loss from inside the network are becoming increasingly available. Some come from the network security or management software worlds; a few are brand-new forays by startups that exist specifically to address the problem.

Even the most sophisticated technology can't replace intelligent, risk-aware management, says Philip Cronin, COO of Polar Cove, an information security consultancy in Providence. "[Technology] is not the silver bullet," he says. "The technical part is really the easy part. The people and the [process-

es] are much more difficult to address."

The "people" angle—recruiting and retaining trustworthy employees—is already a goal for most firms. With existing employees, a firm can raise awareness of information-security risks through regular training programs.

Firms may be less likely to have enforced information-security policies in place, simply because they aren't thinking about the security risks inherent in the daily workings of the firm. For example, Cronin says managers should think about how to label and store documents, so that depositions don't end up in the same place as a memo about the firm's holiday party.

Firms should also ensure that human resources keeps the IT department apprised of firings or other sensitive personnel incidents. That way, a fired or departing employee's access to sensitive information is sure to be terminated as he or she is walking out the door. Cronin says it's a less common practice than one might think: "We have seen situations where employees have left organizations and their accounts have been left open for days and days, sometimes even their remote accounts."

Howrey's Brian Conlon says that if it's suspected that someone is up to no good, requests for records for an employee's network and telephone activities go not just to IT, but to human resources and the firm's general counsel as well.

Still, be careful not to go overboard. Too many restrictions on what employees can do from their own computers can hamper productivity or alienate employees, cautions Baker Robbins' Zawa. He says no useable security system will ever be foolproof: "The systems engineers who get the call in the middle of the night to fix something on a server need access. So there's a delicate trade-off there." **LF**

Lorelei Laird is a freelance writer based in Los Angeles. E-mail: llaird@aberrant.org.