JUNE 2011

LTN

LAW TECHNOLOGY NEWS

CATCH ME *IF YOU CAN*

Insider trading: Can CIOs protect data when the thief is on the payroll?

MOBILE LAWYER

- 4 printers and 6 scanners reviewed
- Firms embrace Quick Response codes

PLUS:

A tool to help coax peak performance from applications across your network

Sage technology advice for courts facing severe budget cuts

An ALM Publication

CATCH ME IF YOU CAN

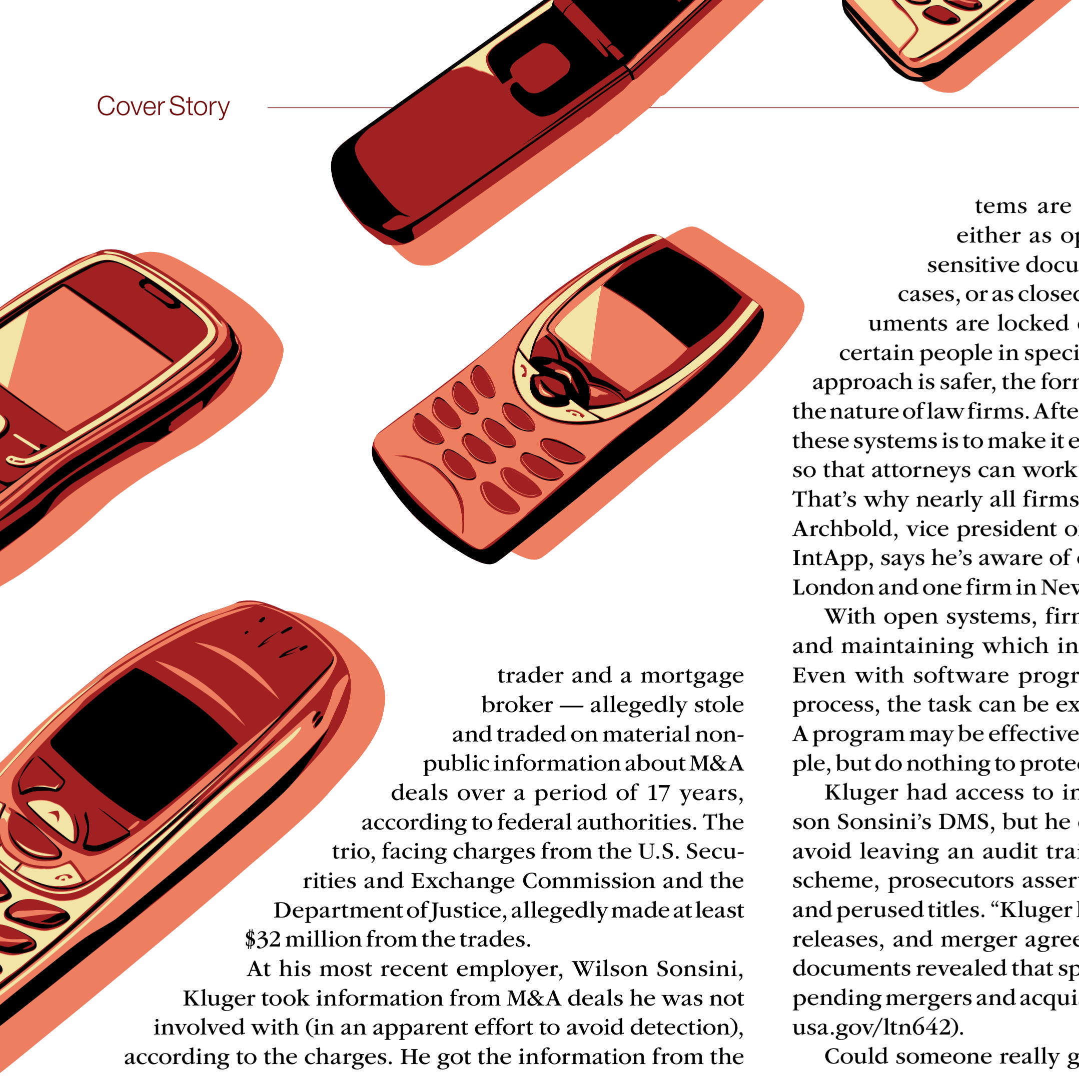
How can you guard your clients' information when the thief is one of your own?

[By Tam Harbert]

Could Matthew Kluger, a mergers and acquisitions attorney arrested on April 6, 2011 on charges of insider trading, have been caught before he did so much damage? That was the disturbing question CIOs discussed behind closed doors at many law firms this spring. Although it's possible to discover the kind of information theft that Kluger allegedly committed, the odds are stacked against it, say CIOs, software vendors, analysts, and IT security experts. That has law firms increasingly worried. Kluger's is just the latest in a string of law firm insider trading cases over the last two years, but it has ratcheted up the level of concern throughout BigLaw. Perhaps it's because the case involved three of the most respected firms in the world: Cravath, Swaine & Moore; Skadden, Arps, Slate, Meagher & Flom; and Wilson Sonsini Goodrich & Rosati. If it happened to them, it could happen to any law firm.

What, exactly, happened? Kluger and two accomplices — a Wall Street

ILLUSTRATION BY DANIEL HERTZBERG



trader and a mortgage broker — allegedly stole and traded on material nonpublic information about M&A deals over a period of 17 years, according to federal authorities. The trio, facing charges from the U.S. Securities and Exchange Commission and the Department of Justice, allegedly made at least $32 million from the trades.

At his most recent employer, Wilson Sonsini, Kluger took information from M&A deals he was not involved with (in an apparent effort to avoid detection), according to the charges. He got the information from the firm's document management system (DMS), say prosecutors.

"What makes this case interesting is that it gets right to the center of information and how law firms manage it," says Adam Hansen, director, information security at SNR Denton U.S.

The case highlights three information security challenges for law firms. First is striking the right balance between the need for security and the need to share knowledge among attorneys. Second is how crucial it is for firms to have not only detailed and clearly thought-out security policies, but also to put the right people in place — with enough authority to implement and enforce them, monitor compliance, and continually review and update the protocols. Finally, the incident shows how firms should pay more attention to threats from insiders.

Not surprisingly, many law firm lawyers, executives, and IT leaders were unwilling to comment on the record for this article, for fear of alienating existing relationships with the three affected firms or exposing their own vulnerabilities.

The divide between IT and lawyers is difficult to bridge.

But the dilemmas are obvious. The service that law firms sell is their expertise and experience. So, by their very nature, firms encourage attorneys to collaborate and share knowledge. At the same time, they have to protect clients' confidential information. In information systems, that tension often shows up in how document and knowledge management systems are configured. They can be set up either as open systems by default, whereby sensitive documents are secured only in specific cases, or as closed systems by default, where all documents are locked down and made available only to certain people in specific circumstances. While the latter approach is safer, the former approach is more conducive to the nature of law firms. After all, the reason most firms adopted these systems is to make it easier to find and share information so that attorneys can work more intelligently and efficiently. That's why nearly all firms leave their systems open. Patrick Archbold, vice president of the risk management practice at IntApp, says he's aware of only two (one Magic Circle firm in London and one firm in New York) that have closed systems.

With open systems, firms must be vigilant in identifying and maintaining which information must be locked down. Even with software programs that can help automate this process, the task can be expensive, complex, and confusing. A program may be effective at creating ethical walls, for example, but do nothing to protect against a rogue insider.

Kluger had access to information on M&A deals in Wilson Sonsini's DMS, but he did not open the documents — to avoid leaving an audit trail that could possibly expose the scheme, prosecutors assert. Instead, he conducted searches and perused titles. "Kluger looked for board resolutions, press releases, and merger agreements because the titles of these documents revealed that specific companies were involved in pending mergers and acquisitions," the charges state (http://1.usa.gov/ltn642).

Could someone really get that much information without opening the documents? "Easy," says George Rudoy,* CEO of Integrated Legal Technology. "Even with all the effort of organizing ethical walls, I have not heard nor seen firms locking the title of the documents. If you go directly into the document management system, you can read all the titles and in most cases you can read short descriptions even if the document is locked." Remember, when people fill out the titles of documents, they are thinking about how to make the document easier to find, not about how to conceal information. Even if the firm uses code names, as was the case in the Wilson Sonsini files, it's often easy to figure out the codes.

One way to keep documents — titles, abstracts, and all — completely out of view is to use a sophisticated search tool such as Recommind's namesake software, which can deep-six information, says Rudoy. The trick, however, is in how you configure and implement the tool. Which systems should the tool be allowed to search? Classifying access rights is a key challenge.

The charges say Kluger also used unspecified "other information." Perhaps he accessed records management or litigation support systems, or overheard conversations and put two and two together. One attorney at a global firm, who spoke on condition of anonymity, says he knew a big deal was afoot at his firm when several professionals were called to a secret meeting at an undisclosed location. He had a hunch that it might involve a particular client, and confirmed it when he noticed in the time management system that those individuals had all billed the time to the same client.

"Somebody who's alert can find little bits of data that by themselves are meaningless, but if you have the background and can put them all together, they add up to a piece of restricted information," Rudoy says.

That's why piecemeal approaches to security are ineffective, say many experts. Most firms have a security policy, but its comprehensiveness, implementation, and enforcement can vary widely. That's because of a disconnect between management and IT that creates a vacuum, say many. Bad things can happen in that vacuum.

Law firm managers understand the intricacies of what data needs to be protected and why, but are not accustomed to thinking in terms of how to use technology to protect that information, says Michael Arkfeld,* president of Arkfeld & Associates. They tend to leave the technology to the IT department. On the other hand, the IT department knows what the technology can do, but typically doesn't fully understand what data needs protecting, from whom, and why. IT people usually think about security in terms of maintaining adequate firewalls and protecting data from outside hackers. The divide has always been very difficult to bridge, says Arkfeld. "It's so prev-

LIKE A HOLLYWOOD SCRIPT

Attorney Matthew Kluger's trail of alleged malfeasance

On April 6, 2011, U.S. Attorney Paul Fishman announced the arrests of Matthew Kluger, 50, of Oakton, Va., and Garrett Bauer, 43, of New York as the Securities and Exchange Commission simultaneously disclosed its insider trading charges against the pair.

"The subjects in this case allegedly attempted to cover their tracks with tradecraft of which Gordon Gecko [sic] would have been proud, but in the end their downfall was similar; criminal activity has been exposed, professional reputations tarnished, and in the end their own financial assets are the ones placed at risk," said Fishman, referring to the 1987 movie, *Wall Street*.

"They plotted to fly under law enforcement radar by using disposable phones to hide their communications, cash withdrawals to obscure the flow of tainted money, and a middleman to conceal Kluger as the secret source of inside information," said Robert Khuzami, director of the SEC's division of enforcement. "Now, those same schemes and devices serve only to make it clear beyond any doubt that Kluger and Bauer were involved in an illegal scheme."

Bauer, Kluger, and a co-conspirator initially identified as CC-1 began the scheme in 1994, alleged Fishman. (CC-1 was later revealed to be mortgage broker Kenneth Robinson, who pleaded guilty to securities fraud and conspiracy charges.)

Kluger's resume:

- 1994-1997: Cravath, Swaine & Moore (New York), summer associate, then corporate associate.
- 1998-2001: Skadden, Arps, Slate, Meagher & Flom (New York), corporate associate.
- 2005 to 3/11/2011: Wilson Sonsini Goodrich & Rosati, senior associate, M&A department (Washington, D.C.)

(Kluger's public profile on LinkedIn (linkd.in/ltn641b) was live as of press time, but not updated from his brief stint as associate general counsel at Asbury Automotive Group before joining WSGR.)

Wrote Fishman: "While at the law firms, Kluger regularly stole and disclosed to CC-1 material, nonpublic information regarding anticipated corporate mergers and acquisitions on which his firms were working." At Cravath and Skadden, Kluger disclosed information relating to deals on which he personally worked, asserts Fishman. "In an effort to avoid law enforcement detection later in the scheme, Kluger took information which he found primarily by viewing documents on Wilson Sonsini's internal computer system, rather than from deals on which he personally worked."

Bauer provided his two colleagues with their profits in cash, "often tens or hundreds of thousands of dollars ... that Bauer withdrew in multiple transactions from ATM machines," asserted Fishman. After Kluger joined WSGR, they took greater efforts to prevent detection of their insider trading scheme. "They generally only spoke to each other about proposed transactions on pay phones or prepaid cellular phones that they referred to as 'throwaway phones' and purchased with cash. They often got a new phone for each of their insider trading deals," Fishman noted. Bauer "directed CC-1 to burn approximately $175,000 in cash ... out of concern his fingerprints would be found on the money."

Recorded conversations revealed Kluger's expectation that he would be busted: "By the way, I got rid of my computer. I got rid of my iPhone where I had looked up some stock quotes. Those are gone. I mean history. Gone," Kluger is quoted.

"[I]f they start looking at me and look at my bank records and all that other stuff it could be, it could get ugly."

— Monica Bay

Sources: U.S. Securities and Exchange Commission and Department of Justice press releases

Editor's Note: LTN reached out to all three firms for comments for this story. Only Wilson Sonsini offered a statement, from spokesperson Courtney Dorman:

"We were shocked to learn of the conduct the government has alleged a former employee committed against us and two other prominent law firms. We have provided our full support to the federal investigation and will continue to do so. In light of the pending actions by the U.S. Attorney's Office and the S.E.C., we are not in a position to comment further."

alent today. I think it's absolutely the most egregious competency issue facing the U.S. legal profession."

Archbold offers an example. The person in charge of managing ethical conflicts is usually a firm's general counsel. "They hear the word wall or screen and they think ethical wall," which often comes into play when a lateral hire joins the firm. "But insider trading has nothing to do with a lateral issue," he explains. What's needed in many cases is a way to secure the information from all eyes except the handful of attorneys working on that particular matter.

Jack Halprin, vice president, e-discovery and compliance, at Autonomy — which offers Autonomy Interwoven content management systems — urges firms to look to the broader area of information governance. "Focusing on a single event or action will often fail to uncover the fraud or illegal activities," he says. Instead, firms should monitor and understand all interactions to facilitate access to information and provide the necessary compliance controls. "There isn't a specific protocol that a firm could follow to prevent insider trading," says Halprin. "If someone wants to breach their obligations, they will find a means and method to do so. The key is to have policies, people, and technology in place that can help identify the interactions that can uncover the malfeasor. Put context around the scope of the interactions, not a single interaction taken out of context."

INSIDERS

The case of Matthew Kluger and his alleged co-conspirators is just one in a recent string of charges against attorneys or IT managers accused of stealing information and then trading. Here are a few examples from the last two years, with links to related news stories.

APRIL 2011: Canadian regulators expanded previously filed allegations, accusing Mitchell Finkelstein, formerly with Davies Ward Phillips & Vineberg, of illegal trading on information he gained while acting as counsel in several M&A transactions. bit.ly/ltn641c

MARCH 2011: The SEC filed civil charges against Todd Leslie Treadway, who worked as an associate at Dewey & LeBoeuf until 2008. The charges allege that in 2007 and 2008 Treadway made $27,000 in profits trading on information he obtained at Dewey. bit.ly/ltn641d

DECEMBER 2010: The SEC accused Jeffrey J. Temple, former information systems and security manager at Richards Layton & Finger, of engaging in insider trading using the firm's confidential files. The charges say he made more than $182,000 in illegal profits. bit.ly/ltn641e

NOVEMBER 2010: Dominic Côté, a former information technology specialist with Ogilvy Renault in Montreal, agreed to pay more than $1.3 million in fines after pleading guilty to Canadian regulators' charges of trading on insider information he obtained from the law firm's computers. bit.ly/ltn641f

NOVEMBER - DECEMBER 2009: Two lawyers from Ropes & Gray – Brien Santarlas and Arthur Cutillo – as well as Michael Kimelman, who formerly worked as an M&A lawyer at Sullivan & Cromwell, were among those charged with insider trading in connection with the Galleon case. bit.ly/ltn641g

Adopting a more skeptical approach may be the hardest part of improving security at law firms. One BigLaw IT professional, who spoke only on condition of anonymity, suggests the problem of internal miscreants may be overrated: "The fact that such cases are relatively rare is a signal that caution should be used before locking down information so tightly, or tracking access so closely, as to inhibit collaboration within law firms and between firms and their clients." Many firms, he says, showcase interdisciplinary synergies during beauty contests to differentiate themselves from competitors, and may be leery about any limitations.

But are these cases rare? After all, the public only knows about the ones that make the news because of government charges. Without an outside investigation, a firm would first have to catch the insider and, second, make that information public, says Arkfeld. Neither event is likely. Nonetheless, clients — particularly in financial services — are raising the bar. They are specifying in engagement letters that firms allow access to their information strictly on a "need-to-know" basis, says Archbold. Some are even conducting onsite physical audits of their law firms' IT security, he notes. In reaction, firms are starting to hire high-level IT security experts for new positions comparable to chief information security officers at corporations.

Law firms are also facing the fact that their own attorneys — people who are sworn to uphold the law — may be criminals. "For as long as I've been in the profession, firms have assumed ethical conduct on behalf of their employees," says the attorney who requested anonymity. "There is very little in the way of a well-armed compliance function in law firms."

Yet, the threat from insiders "is where our biggest risk lies," says Judith Flournoy,* CIO at Loeb & Loeb. Her firm developed custom software that tracks and logs the activity of each user on the firm's network. "If we see someone repeatedly accessing information or e-mailing or copying a lot of documents, our monitoring system highlights that activity," she explains. "If it looks unusual we notify firm management and management will investigate."

But IntApp's Archbold estimates that only 30 percent of all United States law firms use such technology. Although it can help, it is no panacea, he says. As with all security, its effectiveness depends on how it is implemented, and how much time and resources the IT department can spend on it. It takes a lot of development time and testing to fine-tune a system so that IT is not overwhelmed with false alarms. A lawyer searching through the document system for a precedent, for example, could raise some flags, says Michael Kraft,* general counsel of New York-based Kraft Kennedy. "Do I then go question everybody who looks through the documents searching for precedents?" he asks. "Some of these firms have millions of documents. Look how daunting a task that is."

What's more, even if a firm could lock its IT systems down tight, there are plenty of other ways to ferret out data online. These days anyone with a talent for advanced Google searches, a facility for mining information from social networks such as Twitter and Facebook, and some extra time at his or her home computer could gather "a treasure trove of information," says Craig Carpenter, vice president of marketing at Recommind.

Theodore Banks,* formerly an in-house attorney at Kraft Foods, says he first encountered insider trading problems in the 1980s, when "an associate at one of the major New York firms working on a major transaction decided to profit by cleverly trading in his mother-in-law's account."

Now head of Compliance & Competition Consultants and of counsel to Schoeman Updike & Kaufman, Banks says training and effective employee assistance plans can help firms try to nip malfeasance in the bud. Incoming associates should go through a battery of intense training, including "a signed certification not to trade in securities of any company represented by the firm, or on the other side of a deal," he says.

But if an attorney is a crook, no amount of signed documents will do any good. Kluger had signed Wilson Sonsini's policy which clearly prohibited insider trading and included a penalties section in bold type, according to charges. (See *LTN* web version of this article: law technologynews.com.)

Firms need a better "understanding of the behavioral factors that would cause people to do these stupid things," says Banks. Firms should confront workplace issues, such as excessive hours or abusive bosses, "that might trigger a desire to exact revenge." Also, establishing employee assistance programs, affiliations with credit unions, and an emergency loan program can help employees resist temptation, he says. "Bottom line is that human nature is not perfect, but law firms generally are poor managers of their staff."

TAM HARBERT DISCUSSES BIGLAW INSIDER TRADING
VIDEO: http://bit.ly/ltn6p43 PODCAST: lawtechnologynow.com

In the end, behavior depends on ethics and morals. Flournoy, for one, thinks it may be time for firms to re-emphasize ethics, with training and mentoring. "There is only so much technology can do to enforce behavior," she says. "And if we begin to think that [technology] is the answer to the dilemma, I fear we are going to miss the most important question of all, which is, 'Why did this guy think it was OK to do this?' "

**Member, LTN Editorial Advisory Board*

Tam Harbert is a freelance reporter based in Washington, D.C. E-mail: tam@tamharbert.com.

BATTENING DOWN THE SECURITY HATCHES

Tight security relies on three key supports, say IT security experts: processes, technology, and people. Here are some best practices:

PROCESS: Design detailed security policies and procedures, document them, and educate your staff.
Conduct regular risk assessments to identify and review what information and documents need to be protected, where they are located, which people are allowed access, and what procedures and technology are required to ensure protection.
Roll out new security technology gradually, stress-testing it along the way to make sure it works as intended.

TECHNOLOGY: Use software that includes the ability to wall off sensitive information from general search, including document titles and summaries.
Use software that logs and monitors user activity on the network. It not only helps you track what is being accessed, but also creates an audit trail.
Encrypt sensitive documents and e-mail, and use two-factor authentication for any remote access.

PEOPLE: Create a senior-level position with responsibility specifically for IT security.
Assign IT staff to audit logs regularly and to investigate any alerts promptly.
Institute formal training to remind attorneys of ethical duties and to educate them on the security policies and procedures of the firm. Stress not only why adherence to security procedures protects the firm and its clients, but also spell out the consequences for individuals who violate the rules.
Formalize mentoring programs to instill strong ethics and security awareness for new associates and lateral hires. — T.H.