From the Pittsburgh Business Times
:http://www.bizjournals.com/pittsburgh/print-edition/2014/11/14/cyberthreats-prompting-firms-to-tighten-access-to.html

Cyberthreats prompting firms to tighten access to clients' records

SUBSCRIBER CONTENT: Nov 14, 2014, 6:00am EST

Patty Tascarella
Senior Reporter- *Pittsburgh Business Times*
Email | Twitter | Google+ | LinkedIn

In September, an information technology specialist at a prominent Silicon Valley law firm was arrested and charged by the FBI with insider trading. It marked the second time in two years an employee at Wilson Sonsini Goodrich & Rosati PC had been busted for a similar crime.

Cyberthreats such as this illustrate the threats that can come from inside and out, and Pittsburgh-area law firms have stepped up their vigilance accordingly.

"There have been a number of recent higher-profile

cases where employee theft has been an issue for technology and trade secrets information and, of course in today's environment, there's always the concern of hackers accessing databases," said Kirk Miles, director and vice president at The Webb Law Firm. "It's something we as a firm recognize as a concern because our clients do trust their technology with us and we try to protect that by making sure our systems are secure."

Steps that law firms can take to ensure their data remains safe include the use of firewalls, secure data backups, encryption of confidential information, electronic audit trail procedures that track who is accessing confidential data and training employees who use external access portals on password protection and other security policies.

"We have given significant and careful consideration to the issue and have taken appropriate safeguarding steps," said George Stewart III, Pittsburgh managing partner at **Reed Smith LLP**, Pittsburgh's 10th largest private company. "We have technology safeguards and continuous training in place to help us avoid these situations."

Understandably, many local firms, including Reed Smith, are not willing to disclose the details of their strategy to protect client information.

However, few would disagree that law firms — and their clients — are increasingly vulnerable to technology and information breaches and even combinations of the two.

"As you can imagine, law firms face an array of cyberthreats on a daily basis," said Timothy Ryan, CEO of **Eckert Seamans Cherin & Mellott**, Pittsburgh's fourth-largest law firm.

"Firms have prophylactic and technical protections in place to handle those situations as they arise," he continued. "Inside jobs, like the situations at Wilson Sonsini, are fortunately less common. Nonetheless, law firms need to put pre-emptive practices in place and take the utmost care to avoid the misappropriation and exploitation of sensitive, confidential client information. The value of the data law firms house on behalf of clients is immeasurable, and the industry's very integrity is staked on the protection of that information."

Miles said The Webb Law Firm has a state-of-the-art IT system providing appropriate safeguards and protection.

"In addition, we have a very secure office environment with file records locked down electronically so that outsiders cannot get in and only employees through password protection can get into our databases and access our client information," he said. "All of our files and our office environment are appropriately secure. Only employees with key cards can access our nonpublic spaces."

In some cases, the changes being implemented at law firms are the result of industry directives. The **Pennsylvania Bar Association's** committee on legal ethics has issued several opinions to help guide law firms on how to protect clients' confidential information.

For example, word processing programs such as Microsoft Word use meta data to preserve a document's revision history, said James Singer, partner and chair of the intellectual property department at **Fox Rothschild** LLP. This history can include comments and notations that are confidential and not intended for public release. Five years ago, the PBA issued an opinion stating attorneys have a duty to use reasonable care in removing client-sensitive meta data from documents before sending them to a third party.

Similarly, the PBA in 2012 issued an opinion stating law firms must use reasonable care when making data available to employees via cloud computing.

Eckert Seamans has avoided moving to cloud-based storage for security reasons.

"Many of our protocols are based on strictly limiting who can access what information," Ryan said. "As CEO of the firm, even I can't access most of our folders and files on the system. Only the select few who are working with the client on a particular matter with a need to know can access the information."

Volume raises risks

Jacob Rooksby, assistant professor at **Duquesne University** School of Law, said security has taken on new importance as the administrative structure of large firms has grown and

the management of confidential data often is handled in its own silo, separated from day-to-day attorney oversight.

"These concerns are only heightened as increases in data volume and the search for economies of scale has led firms to use cloud-based storage options and engage with more third-party vendors in the IT space," Rooksby said. "As more people come into contact with sensitive data, and as storage shifts from the file room to an e-room or other virtual location, the potential for breaches and leaks increases."

That puts firms of all sizes on alert.

Just ask Patricia Dodge, managing partner of Meyer, Unkovic & Scott LLP, which has about 56 lawyers based downtown but serves clients who operate internationally.

"I've talked to managing partners at much larger firms in town and get the sense that they're probably asked more often by their clients to do many more things than we've experienced to date, but that day is coming and we're trying to be ahead of the curve," Dodge said. "We can't predict what the client will want, but we want them to know we can do it. You've got to think in a different way than the traditional methods. There are more challenges to keeping a client's secrets secret."

With respect to its paper file documents, Meyer Unkovic moved those to a central file room where everything is barcoded and the access is limited.

"You can't just walk in and take a file. You've got to have a reason," Dodge said.

More recently, Meyer Unkovic has been approached by some clients who want to have a dedicated and secure room just for their materials.

Meyer Unkovic is redoing its space and considering "adding a secure room for certain client files" as part of the remodeling, Dodge said.

"There are other requirements about how they want us to keep their paper files," Dodge said. "Not everyone has the same structure or wants things done the same way, so you've got to figure out how to employ all these different systems within your office structure."

She added: "We've got to look at each one and address it individually. We want them to be completely comfortable with our ability to handle their sensitive information."

The firm has a technology committee and what Dodge described as "a very robust" IT department, both of which are continually challenged to keep up to date with the best ways to address security issues.

"Right now, we're looking at some new software and encryption strategies we may want to use," Dodge said. "Our document management system has security features for our documents online and emails and other electronic communications so we can limit access to information that's sensitive or confidential."

Many clients are requiring their lawyers to undergo cybersecurity audits as a condition of receiving work, said Singer of Fox Rothschild. This is especially common in the financial sector because regulators are pressuring banks to ensure data security.

"The banks are in turn directing that pressure to their vendors — including law firms," Singer said. "The banks not only require law firms to comply with specific data security procedures, they also are auditing the firms' compliance with those procedures."

Ryan said Eckert Seamans is frequently asked by clients — often in regulated sectors such as financial services and health care — to participate in comprehensive data security audits.

Recruiting process affected

The concern about the potential for insider trading and other breaches begins even before a lawyer is hired. In today's security-conscious environment, firms are getting pickier about who they hire at the partner level, according to Lori Carpenter, president of recruitment firm Carpenter Legal Search.

"Ten years ago, if I sent a partner with a $2 million or $3 million book of business to a firm, they (the potential employer) were always excited right out of the gate," she said. "That's not the case now. They've become a lot more discerning, really zeroing in on who they (the potential employees) are as people. Increasingly, it's been an evolution in terms of the process of hiring partners. We've seen more and more partners who must sign confidentiality agreements, most often before receiving an offer."

Eckert Seamans conducts tough background checks, and job candidates must sign insider trading and confidentiality policies upon accepting an offer of employment.

"And they're re-inked on a yearly basis thereafter," Ryan said. "These policies also help ensure that honest personnel know how to report any suspicious activity to our seasoned HR professionals."

Still, Singer believes law firms are less likely to have as many large-scale data breaches as consumer-oriented companies.

"A reason for this may be that law firms have fewer points of access for hackers," he said. "We don't have point-of-sale credit-card readers, online shopping carts or other consumer-facing portals that can be breached.

"On the other hand, when it comes to safeguarding confidential information from unauthorized internal access, law firms face many of the same issues that other companies do," Singer said. "Just as a consumer-facing business may hold confidential data about thousands of consumers, a large law firm may hold proprietary and sensitive information about thousands of its clients."

Despite the high-tech solutions, there's always the danger that information can escape the old-fashioned way — through loose lips, a growing concern when many people have private conversations on cell phones in public areas.

"We are also vigilant in matters such as discouraging water-cooler chatter about client issues, quickly retrieving printed documents from our printing centers and so on," Ryan said.

Patty Tascarella covers accounting, banking, finance, legal, marketing and advertising and foundations. Contact her at ptascarella@bizjournals.com or 412-208-3832. .