

Data Security Takes A Backseat At Law Firms

By Erin Coe

Law360, New York (June 03, 2010) -- When Sharon Nelson, president of information technology support provider Sensei Enterprises Inc., meets with law firms for the first time to review their safeguards against a data breach, she often finds an environment with more security holes than security walls.

“Law firms want faster machines and upgraded software, but security tends to hobble painfully far behind. There’s a sense that until a breach happens to you, it can’t happen here,” she said.

Holding gold mines of confidential client information, law firms are becoming popular targets for cyber attacks, yet many firms continue to scrimp on devoting resources toward stepping up their information technology systems, according to experts.

Over the past five years, sophisticated cyber attackers have expanded their intrusions at government and defense-related targets to go after researchers, manufacturers, nonprofits and law firms, according to a January report by information security firm Mandiant Corp.

“We’re seeing security events, such as network intrusions, in which attackers breach the security environment through the Internet and have access to the information in it,” said Stephen Surdu, Mandiant’s vice president of professional services.

The data that law firms keep covers an array of Social Security and bank account numbers, medical records, financial transactions, sensitive and embarrassing company memos, mergers and acquisitions, and intellectual property — all of which could be a jackpot for a competitor, employee, foreign government or hacker bent on misusing, selling or leaking the information.

“If a party is trying to get valuable information, law firms are one of the links in the information chain and are therefore attacked,” said David Isom, founder of Isom Law Firm that focuses on electronic discovery and digital law.

Cyber attackers may also strike law firms because they organize information better than their clients, according to Surdu.

“Certain information may be harder to find all in one place in a particular organization, but if someone is interested in a particular topic, it may be more straightforward to find it at a law firm,” he said.

Mandiant has worked with more than 50 law firms dealing with issues including confirmed or suspected breaches, and many of the firms tend to have clients or cases in China.

“We are seeing a lot of attacks emanating from the Asian area,” Surdu said. “Firms may be representing clients that produce tools or software that are of interest to that part of the world and are a greater target.”

The FBI issued an advisory in November 2009 that more hackers were using complex e-mail schemes, known as spear phishing, to go after information held by U.S. law firms.

The agency said at the time that network defenses against these attacks could be difficult because they appeared to come from a trusted source and “the subject lines are spoofed, or crafted, in such a way to uniquely engage recipients with content appropriate to their specific business interests.”

Gipson Hoffman & Pancione, a Los Angeles-based law firm, became the target of that kind of scheme earlier this year.

Shortly after the firm launched a \$2.2 billion copyright infringement suit on behalf of CYBERSitter LLC in January, the law firm noticed an unprecedented spike in suspicious e-mails.

The e-mails looked like they had been sent from lawyers at the firm using their real e-mail addresses and included a message urging the recipient to click on an attachment. But an internal investigation revealed that the attachment carried malware that appeared to be coming from China, according to Elliot B. Gipson, one of the attorneys representing CYBERSitter.

Fortunately, lawyers and staff at the firm had been warned to watch out for questionable e-mails following the filing of the suit, which accused the Chinese government and several companies of stealing code from CYBERSitter's Internet filtering program, and they were able to avoid making the mistake of clicking on any attachments, Gipson said.

“The suit deals with IP theft with allegations against the People’s Republic of China and Chinese companies. It seemed like a no-brainer to make everyone at the firm aware that there might be an attack,” Gipson said.

While it may be a no-brainer for some, many firms of all sizes have been slow to ramp up their security measures and are leaving themselves open to attacks, according to experts.

“Regional and boutique firms have valuable information, but they do not have the level of security in place like large firms. Meanwhile, large firms move on square wheels and are not very efficient,” Nelson said.

As service organizations, law firms have not placed the same premium on their internal systems as have Fortune 100 and 500 companies.

“With document storage and management, there is oftentimes an attitude by law firms that they will put an infrastructure in place as long as it does not impede their ability to serve their clients. But those two things may be at odds with one another,” Surdu said.

Law firms are simply not devoting enough money and staff to protecting their information, according to Alex Stamos, a co-founder of security consulting firm iSEC Partners Inc.

Stamos said he has never met a law firm with a team dedicated to securing its data infrastructure, and without such a team, a breach could occur without a firm even realizing it.

“Going after law firms may be much easier than targeting companies themselves. Law firms seem pretty stingy on information technology expenditures,” he said.

Instead of ramping up security practices across the board, a law firm may focus on boosting IT measures for a specific transaction for a client, according to Isom.

“The firm may use encryption for a big project, but it won’t do this on a firmwide basis because of the costs and because it doesn’t want to mess with security measures and encryption adopted in other matters,” he said.

Law firms have not been very diligent about doing vulnerability assessments of their security environment, and they need to check on firewalls, configuration settings on servers and source codes on Web applications, as well as make sure that their systems are properly updated, Surdu said.

While many firms concentrate efforts on protecting their computer network, they tend to forget that mobile devices like laptops, smartphones and iPhones, as well as social media sites, can carry risks, according to Nelson.

“iPhones are insecure devices and should not be used for business purposes,” she said. “They are easily penetrable by someone with minimal technical skills.”

Networking sites like Facebook may be used for firm marketing, but users can add different third-party applications that may not be secure, and firms should adopt a social media policy for using these sites, according to Nelson.

In addition, law firms would be wise to inform clients in policies, engagement contracts and notices on their Web pages about the flaws inherent in information security systems, according to Benjamin Wright, a technology attorney and a senior instructor at The SANS Institute, which provides computer security training.

“I believe the expectations for security of information by the public today exceed reality,” he said. “A perfect information security system does not exist. There is a degree of risk to sharing any information today.”

While firms cannot prevent a cyber attack, lawyers and staff can be more aware of the red flags to avoid being duped by one, according to Gipson.

“You’ve got to listen to your gut. It’s better to waste a couple of minutes not opening an e-mail than clicking on an attachment and finding out later that you’ve downloaded a virus. At best, it’s

just an annoying virus, but at worst, you could be making embarrassing phone calls to people,” he said.

At the same time, law firms have an ethical duty to preserve confidentiality and are expected to protect the sensitive information they receive, Wright said.

“Law firms are held to a high standard of care in terms of information security,” Wright said. “It’s inherent in the practice of law for clients to give them their most intimate secrets, and it’s natural that clients would expect a high degree of security at law firms.”