UT LAW CLE THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

40th Annual Civil Litigation Conference

October 27-28, 2016

Austin, Texas

CYBER SECURITY:
What lawyers and law firms need to know about data security to avoid losing clients and getting sued

Michael C. Smith
Rob King

Michael C. Smith
Siebman, Burg, Phillips & Smith, LLP
Marshall, Texas
michaelsmith@siebman.com
903-938-8900

Rob King
Corporate IP Counsel
Silicon Labs
Austin, Texas
512-416-8500

Law firms are becoming big business for hackers. In many law firms, data has migrated from paper to electronic form, and that, combined with the fact that many of the law firms which deal in significant sums of money have numerous locations and require online access around the clock, means that entry points for hackers have multiplied exponentially in recent years. And this is valuable information. Bradford Bleier, unit chief for the FBI's cyber division has said that "[l]aw firms are tremendous concentrations of really critical, private information. [Infiltrating those computer systems] is a really optimal way to obtain economic and personal information."

Unfortunately, law firms' defenses against such cyber attacks have not kept pace. Most law firms do not have even basic cyber security controls in place for detecting or responding to data breaches. And lawyers and their staff often have habits that unknowingly assist hackers in breaching what security measures may exist.

I. Data Breaches at Law Firms

In recent years, numerous law firms, large and small, have been the victims of data breaches. Beginning in 2008, reports began to circulate of law firms being hacked. In some cases the firms in question had been involved in litigation involving China, raising concerns that the hackers were based there. In November 2009, the FBI issued an advisory that warned companies of "noticeable increases" in efforts to hack into law firm computer systems. Firms were particularly cautioned to be aware of "spear-fishing" attacks.

A 2012 study from the security firm Mandiant Corporation reported that 80 percent of the nation's 100 largest firms were victims of hacking. In 2015, an American Bar Association survey revealed that even though 15% of law firms, and one in four of firms with at least 100 lawyers, had fallen victim to a breach, nearly half had no response plan. Most lacked security measures beyond rudimentary tools like firewall software, spam filters and virus scanners. This despite the fact that Cisco's 2015 annual security report named laws firms as the seventh highest target for cyber criminals in the previous year. And, earlier this year, the FBI's cyber division issued an alert that hackers appeared to be specifically targeting international law firms as part of an insider trading scheme, including law firms Cravath, Swaine & Moore and Weil, Gotshal & Manges, L.L.P. Perhaps the most widely publicized cyber-attack on a law firm was the Mossack Fonseca "Panama Papers" data breach, in which the leaked information illustrated a global network of shell companies used in tax evasion schemes. More than 2.6 terabytes of data, including 11.5 million sensitive records were stolen, without the firm being aware of the theft.

But cyber threats are not limited to large firms engaged in multibillion-dollar M&A deals. Just this summer, the small Clarendon, Texas law office of James Shelton began receiving thousands of calls a day from across the U.S., Canada, and the United Kingdom. Apparently, hackers had used one of the law firm's email accounts to message recipients with the subject line "lawsuit subpoena." The company-specific email asked if the legal department had received the subpoena yet, and included an attachment with malware that infects systems, steals banking credentials, and accesses financial records. The firm immediately disabled the email account and posted a warning on its website advising against clicking any links or downloading any attachments.

Why are law firms a target? First, hackers are drawn by the sheer quantity and quality of valuable documents, such as descriptions of technical secrets, business strategies, and due

diligence material on transactions, financing, and mergers. Second, data thieves may target law firms as a way of filtering out low-value information. Although large corporations store large amounts of data, outside counsel usually keeps a smaller, more carefully selected and organized set of documents. Finally, firms often have worse data security than their clients. As cybersecurity and data protection attorney Shawn Tuma of Frisco's Scheef & Stone has observed, lawyers are under significant pressure to do things quickly and efficiently, which makes it difficult for IT teams to install robust security systems. In addition, lawyers are always interested in emails seeking to hire them to handle cases making reading and clicking on emails from strangers a semi-routine occurrence in the law firm environment.

What is the risk? Law firms with lax cybersecurity risk more than just the loss of a client; they also risk malpractice exposure and disciplinary actions. In 2012, the ABA updated its model rules of professional responsibility, requiring lawyers to make "reasonable efforts" to prevent the disclosure of and unauthorized access to client information. Many states similarly have adopted more modern standards, either for lawyers or in the form of "personally identifiable information" (PII) laws. And clients are taking note. As recently as April, a New York real estate lawyer, Patricia Doran, was sued by two clients who allege that her use of a "notoriously vulnerable" AOL email account resulted in their loss of nearly $2 million. According to the lawsuit, Doran's computer negligence allowed hackers to not only read all of the lawyers emails, but also to impersonate the attorney for the sellers of real estate that the couple was buying. Doran allegedly forwarded bogus emails from the hackers to her clients, resulting in funds being wired to unauthorized accounts.

II. What Puts Firms at Risk

There are several activities or tendencies that put law firms at risk of cyber attacks.

1. Clicking on Unsafe Attachments

The single worst behavior from a cyber security perspective is clicking on unsafe attachments. A recent study by researchers at the Friedrich-Alexander University (FAU) of Erlangen-Nuremberg in Germany found that about half of the subjects in an experiment click on links from strangers in emails and Facebook messages despite claiming that they were aware of the risks.

There are a number of characteristics that dangerous emails may have:

a. Vagueness

An email that purports to be from an institution that should know you but that uses a generic greeting, such as "dear customer" and makes only generic references to your business or account should be a red flag. Broken English, grammatical errors and bizarre wording are also good indicators of a fraudulent email scheme.

b. Capitalizing on high-profile news/disasters

Unsolicited emails that purport to be from charities dealing with natural disasters are another good candidate for a fraudulent email scheme. Snopes.com has a list of fake charities, and is a good source to see if the email received is just another email scam.

UT LAW CLE | THE UNIVERSITY OF TEXAS | TEXASLAW

Find the full text of this and thousands of other resources from leading experts in dozens of legal practice areas in the UT Law CLE eLibrary (utcle.org/elibrary)

Title search: Cyber Security: What Lawyers and Law Firms Need to Know About Data Security to Avoid Losing Clients and Getting Sued

Also available as part of the eCourse
2016 Page Keeton Civil Litigation eConference

First appeared as part of the conference materials for the
40th Annual Page Keeton Civil Litigation Conference session
"Cybersecurity for Law Firms"