JOHN F. MARSH

Are You the Weakest Link? As Hackers Target Law Firms for Confidential Information, Lawyers Need To Be Vigilant

It seems like with each passing day there is a new headline about yet another cyber-attack or hacking incident targeting a bank, a security firm, or another business that is using or storing highly confidential information. Unfortunately, it appears that lawyers are now becoming a favored target.

One reason for these increasing attacks directed at law firms is the fact that lawyers are "high value" targets who may have sensitive transactional information for multiple clients. As a result, there has been a greater number of reports of efforts by hackers to attack system networks of large law firms to cull confidential data on sensitive deals and transactions.[1] These attacks have been sufficiently serious that the Federal Bureau of Investigation's Cyber Division convened a meeting with representatives of the top 200 law firms in New York City in November 2011 to address the rising number of intrusions into law firms' systems.

One attack that gave rise to the FBI's concern involved China-based hackers who had attempted to derail an Australian mining conglomerate's $40 billion acquisition of the world's largest potash producer. The hackers "zeroed in on offices on Toronto's Bay Street, home of the Canadian law firms handling the deal." According to Bloomberg News,

> Over a few months beginning in September 2010, the hackers rifled one secure computer network after the next, eventually hitting seven different law firms as well as Canada's Finance Ministry and the Treasury Board, according to Daniel Tobok, president of Toronto-based Digital Wyzdom. His cybersecurity company was hired by the law firms to assist in the probe. The investigation linked the intrusions to a Chinese effort to scuttle the takeover of Potash Corp. of Saskatchewan Inc. by BHP Billiton Ltd. as part of the global competition for natural resources, Tobok said. Such stolen data can be worth tens of millions of dollars and give the party who possesses it an unfair advantage in deal negotiations, he said.[2]

Why are law firms being targeted now? Special Agent Mary Galligan, the head of the FBI's Cyber Division in New York, believes that, "as financial institutions in New York City and the world become stronger, a hacker can hit a law firm and it's a much, much easier quarry." Therefore, Special Agent Galligan's unit held the meeting with the 200 law firms in New York. "We told them they need a diagram of their network; they need to know how computer logs are kept," Special Agent Galligan said of the meeting. "Some were really well prepared; others didn't know what we were talking about." Mandiant, a cybersecurity firm based in Alexandria, Va., estimates that the computer networks of 80 U.S. law firms were hacked last year.[3]

The search for confidential transactional or client information is not the only reason that hackers may target law firms. Representing an unpopular client may also trigger a cyber-attack. For example, the law firm of Puckett & Faraj, which represented a Marine accused of killing 24 Iraqi civilians in 2005, was recently targeted by hackers associated with the group named Anonymous. After the firm secured a favorable plea arrangement for the Marine, Anonymous raided the firm's site and boasted that it stole "court mails, faxes, transcriptions, etc."[4]

How can lawyers protect themselves? Cybercriminals use a number of different approaches to gain access to attorneys and law firms. Perhaps the most identifiable approach is what is known as "spear phishing" or "whaling"—targeted attacks directed at particular employees within an organization seeking unauthorized access to confidential data or trade secrets.

In order to succeed, spear phishing requires three things:

- The supposed source must appear to be a known and trusted individual.
- The source must supply information within the e-mail that validates that the source is who he/she claims to be.
- The request being made must seem to make sense to the recipient.[5]

To accomplish this kind of attack, the perpetrators will troll for publicly available information on the Internet in order to build digital dossiers on the attorneys they target. This process has become known

as "social engineering," and, in the age of LinkedIn, Facebook, and Twitter, the details of a potential target's career and responsibilities now are on the Web for all to see—and for some to misuse in an e-mail that may sound more credible because it incorporates some of that information.

Junior or inexperienced associates are not the only ones that can be duped; senior executives and partners at law firms are just as susceptible and perhaps even more so. To illustrate, in 2008, nearly 1,800 senior executives took the bait of messages masquerading as official subpoenas requiring the executives to appear before federal grand juries. The e-mails correctly addressed the firms' chief executive officers and other high-ranking executives by their full name and included their phone numbers and the companies' names. Recipients who clicked on a link that offered a more detailed copy of the subpoena were taken to a website that informed them they had to install a browser add-on in order to read the document. When they clicked "yes," a backdoor and key-logging software was installed that stole log-in credentials used on websites of banks and other sensitive organizations. This practice of targeting high-profile recipients is better known as "harpooning" or "whaling."

Mobile devices are also increasingly a gateway for hacking and attacks. For this reason, at the November 2011 meeting, the FBI also recommended that the law firms review their mobility policies, including the security of e-mail linkups and mobile phones. Those firms that have not yet done so should have their lawyers take the following practical steps to protect their work and personal data:

- Make sure employees protect access to their device with a password or PIN to keep intruders out if the device is lost or stolen.
- Download applications only from well-known, trusted sites.
- Make sure employees install system updates and run anti-malware programs as prompted.
- Back up data on a regular basis.
- Have the ability to track any phone and remotely delete all its data if it is stolen. Apps that will allow a user to do this are easy to find.[6]

In sum, intellectual property lawyers frequently advise their clients that it is important to manage and protect sensitive information by, among other things, limiting access, limiting use of encryption, implementing sound security policies, and creating a culture of security. To the extent that law firms are managing highly sensitive technical data or are involved in highly sensitive transactions, they need to heed their own advice and apply it to their employees and to their own information technology networks. **TFL**

John F. Marsh is a partner with the Columbus, Ohio office of Hahn Loeser & Parks, LLP. He is a frequent speaker and blogger (www.tradesecretlitigator.com) on trade secret, covenant not to compete, and cybersecurity law issues. He can be reached at jmarsh@hahnlaw.com or (614) 233-5102.

Endnotes

[1] *China-Based Hackers Target Law Firms to Get Secret Deal Data* (Jan. 31, 2012), available at www.bloomberg.com/news/2012-01-31/china-based-hackers-target-law-firms.html.

[2] *Id.*

[3] *Id.*

[4] *Anonymous Raids Law Firm Over Its Defense of Marine* (Feb. 3, 2012), available at www.scmagazine.com/anonymous-raids-law-firm-over-its-defense-of-marine/article/226294/.

[5] *Spear Fishing and Whaling: Will Your Employees Take the Bait and Expose Your Trade Secrets* (Nov. 4, 2012), available at www.hahnloeser.com/tradesecretlitigator/category/Cybersecurity.aspx.

[6] *The Pros and Cons of "Bring Your Own Device"* (Nov. 16, 2011), available at www.forbes.com/sites/ciocentral/2011/11/16/the-pros-and-cons-of-bring-your-own-device/.