dri™
The Voice of the Defense Bar

e-News Technology
The Newsletter of the Technology Committee

December 27, 2013 Volume 8 Issue 2

DRI Resources

Featured Articles

Waging a Cyber War: Law Firms on the Defense

by Amber B. Barlow

In an age when permanent members of the United Nations Security Council are sponsoring cyber-terrorists to hack into United States businesses such as the New York Times, law firms have also become a target of these efforts. The three major industries in America that face the most frequent threats of state-sponsored espionage are financial institutions, pharmaceutical companies, and energy enterprises. These institutions have already instituted strict security regimens. As a result, cyber-terrorists have made an increased focus on exploiting the possible technological weaknesses of the law firms retained by the target companies. Because of these developments, attorneys can no longer get by with saying that they're "just not good with computers."

It is common knowledge that law firms possess proprietary, confidential information within their computer systems which is undoubtedly very valuable to their clients. Indeed, the very information could be the subject of contentious and expensive corporate litigation which is the basis for the firm's representation of the client. This type of data may range from personal information such as Social Security numbers, to corporate financial documents and other materials related to mergers and acquisitions. Given the sensitivity of the data, law firms are at an all-time risk for cyber-security breaches.

Unfortunately, some law firms are not well prepared for attacks from hackers. For example, one law firm handling a $40 billion acquisition of the world's largest producer of potash, which is an alkaline potassium compound, faced Chinese hackers trying to derail the acquisition. This type of data is worth millions to other businesses trying to gain an edge in negotiation power which explains the hackers' tenacity. But, cyber-security breaches are not always so grand in nature.

For instance, an employee may inadvertently leave a laptop, smartphone, or memory stick at a coffee shop. The device could ultimately fall into the hands of a person who decides

Join the DRI Community

In e-News

Committee Leadership

Committee Chair
Chad S. Godwin
Carr Allison
(205) 949-2921
cgodwin@carrallison.com

Committee Vice Chair
Joseph David Cohen
Porter Hedges
(713) 226-6628
jcohen@porterhedges.com

Newsletter Editor
Michele Hale DeShazo
Kuchker Polk Schell
(504) 592-0691
mdeshazo@kuchlerpolk.com

Click to view entire Leadership

Seminar

to use and/or sell the device with stored, sensitive material. More commonly, security breaches occur by a firm employee opening an attachment to a seemingly innocuous e-mail, but the attachment actually allows the hacker to invade the system and quietly gain access to data. Hackers also target websites they believe lawyers will visit. Recently, hackers compromised the website of a set of barristers' chambers. All users who visited the website ultimately gave these hackers access to their company's system.

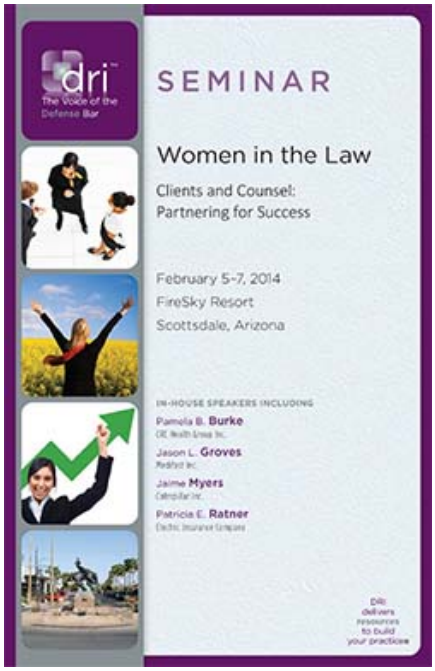
Law firms need to prepare for cyber-security breaches with the emphasis being on a greater awareness of the risk. We are in the paperless age when almost everything is electronic, including many courts' filing systems. With smartphones, iPads, and access to electronic files, lawyers can work from just about anywhere. This allows employees to access secure data within their files from unsecured locations. As technology becomes more readily available to employees in those firms, the increased use of technology unwittingly gives hackers more avenues from which to conduct their cyber assaults.

And, as firms become more aware of hackers, hackers also become savvier. After law firms implement their initial tight cyber-security measures, there must be an understanding that this is not a one-time investment but rather a new reality with a continuing duty.

Beyond just business interests, lawyers also have ethical rules and responsibilities that implicate cyber-security. Cyber-security is an issue that the American Bar Association has addressed with more seriousness. For example, the 2012-2013 President of the American Bar Association, Laurel Bellows stated:

> "We live in a world where our national security is threatened by cyber terrorists, and where private enterprise is forced to respond to cyber theft of intellectual property on a daily basis. The ABA Cyber security Legal Task Force is examining risks posed by criminals, terrorists and nations that seek to steal personal and financial information, disrupt critical infrastructure and wage cyberwar. When our national security and economy are threatened, lawyers will not stand on the sidelines."

According to *Model Rules of Professional Conduct* Rule 1.1 and Rule 1.6, law firms have a duty to protect client information. Rule 1.1, comment [8], provides that a lawyer's professional responsibility is "to maintain the requisite knowledge and skill…including the benefits and risks associated with **relevant technology**…." Therefore, law firms turning a blind eye to potential security issues within their data system create an ethical concern since lawyers are responsible for maintaining their clients' confidential information in such a way that the information is not at risk by being stored through technological means.



Women in the Law

February 5-7, 2014
Scottsdale, Arizona

DRI Publications

Understanding the New E-Discovery Rules

Print to PDF

Rule 1.6(c) states that "a lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." But what happens if there is a security breach and confidential client information is leaked? The commentary found in paragraph 18 of Rule 1.6 says that "the unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of (c) if the lawyer has made reasonable efforts to prevent the access or disclosure." If the law firm had adequate security in place to reasonably protect the information, there would not be an ethical violation.

There are a number of security measures that law firms may use. First and foremost, law firms should have a partner and or senior level attorney designated to oversee technology within the firm in concert with the IT staff. This person would act as the point person if security breaches occur. This individual would be aware of the types of clients that the firm possesses and would set the guidelines for the level of security that should be maintained for each client's file.

Second, law firms should employ IT specialists who constantly monitor and protect the firm's data. Because it is possible for hackers to remain in a law firm's system undetected for a long time, it is almost necessary to have IT personnel in place to regularly police the system. The IT department should be given a budget and be tasked with providing the law firm with the best cyber-security systems for their law firm's client's needs.

Third, the law firm should have a computer usage and technology policy which educates employees, attorneys included, on basic rules, guidelines, and warning signs. Law firms need to articulate clearly to their employees parameters on the use of Wi-Fi, smartphones, memory sticks, e-mail accounts, social networking, and working remotely.

Fourth, the law firm should have a plan in place to handle such possible attacks from the lowest to the highest level. This will help the firm and its employees know how to react if faced with a data breach and will give an indication of whether or not the firm is truly prepared.

Law firms should be aware of the cyber wars that hackers are waging and be prepared to face such attacks. Gone are the days in which law firms can turn a blind eye to their cyber-security.

Amber B. Barlow *is an Associate Attorney with the New Orleans office of Kuchler Polk Schell Weiner & Richeson, LLC, where she practices in the areas of toxic tort litigation focusing on products and premises liability and general civil litigation.*

Back...