CHICAGOLAWBULLETIN.COM

Serving Chicago's legal community for 160 years

MONDAY, AUGUST 3, 2015

Chicago Daily Law Bulletin®

Volume 161, No. 150

Law firms must assess cyber security risks to protect businesses, clients

ALLISON L. WOOD

Allison L. Wood formerly served as a hearing board chair and as litigation counsel with the Illinois Attorney Registration & Disciplinary Commission. She is principal of Legal Ethics Consulting P.C., where she partners with solos and firms to provide preventative ethics counsel as well as ARDC defense. Reach her at aw@legalethicsconsulting.com and follow her on Twitter at @WoodWiseEthics.

About a month ago, I received an e-mail from a close girlfriend. When I clicked on it, there was a message directing me to click on a link to receive a great discount on my next purchase of Viagra. Since I could not imagine why my girlfriend would be promoting the sale of Viagra (or why she would think I would be a good prospect for this product), I concluded correctly that her e-mail account had been hacked and quickly deleted the message.

A few weeks later she sent all of her contacts an apology via e-mail. Whether she took any steps after that to better secure her e-mail account, I don't know.

I imagine many of you have either had your e-mail account hacked or you have been the recipient of an e-mail where the sender's account had been hacked.

Sometimes it is an obvious hack and many of us will simply delete the e-mail and move on. Sometimes it is not so obvious and a click on a link or an attachment might compromise your e-mail account or the data you have on your computer.

These risks to your data have the potential to create cyber liability issues for you or your firm. As explained by Karen P. Randall, a partner and chair of the professional liability, cyber security and data privacy groups, with Connell, Foley LLP in New York, "Cyber liability refers to Internet-based risks and those relating to information technology infrastructure and activities. It is a risk posed by conducting business over the Internet, over other networks or using electronic storage technology."

Cyber attacks in the news are so common that it is easy to lose count of them. In December 2013, Target experienced what is considered the largest hack in U.S. corporate history affecting some 40 million customers.

In 2014, Sony Pictures Entertainment was hacked and about 40 gigabytes of sensitive company data from its computers was stolen and posted online. In June 2015, it was reported that China hacked the United States and stole the personal information of 4 million federal employees.

And, in July 2015, it was reported that Ashley Madison, a dating site for married people, was hacked and the exposure of the infidelity of 37 million users is at stake. Of course, some argue that these users deserve to be exposed, but cyber attacks are rarely triggered on the basis of morality.

Lawyers and firms who underestimate the risk of a cyber attack or who fail to take affirmative steps to protect their data, have an increased risk of becoming the subject of a disciplinary or malpractice claim. Rule 1.6 Confidentiality of Information, which prohibits lawyers from revealing confidential client information, also speaks to a lawyer's duty to protect client information.

While not as frequently publicized, law firms have been victims of cyber attacks.

Comment 16 to the rule states that, "A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision." Further, Comment 17 to the rule requires the lawyer to take reasonable precautions to prevent the information from coming into the hands of unintended recipients.

While not as frequently publicized, law firms have been victims of cyber attacks.

In an article published in Bloomberg Businessweek on March 19, 2005, titled, "Cyber Attacks Upend Attorney Client Privilege," the cyber security firm Mandiant reported two examples of cyber attacks on large law firms. Wiley, Rein LLP, a Washington, D.C., law firm was targeted by hackers linked to China's military in connection with a trade dispute it was handling for a maker of solar panels, and McKenna, Long & Aldridge LLP, an international firm with offices in 15 cities, lost Social Security numbers and other employee data when one of its vendors was targeted.

According to an article titled, "The New Law Firm Challenge: Confronting the Rise of Cyber Attacks and Preventing Enhanced Liability" by David Mandell and Karla Schaffer that appeared in Law Practice Today in March 2012 approximately 80 major law firms were victims of cyber attacks in 2011.

To be sure, large law firms are not the only firms at risk. Randall explained it this way: "Although all law firms are increasingly vulnerable to attacks by cyber criminals due to the large amount of highly confidential client data maintained, midsize, boutique and solo firms may be targeted more often because they simply do not have the financial resources available to devote to cyber security."

While some law firms may not have the financial resources to devote to cyber security, some firms may not appreciate the fact that cyber security is a risk management issue that must be addressed by every business.

As Luke Ciciliano, an SEO consultant and technology blogger from Las Vegas who has helped numerous attorneys build their practice through online marketing explains, "Most attorneys don't deal with the business end of things until something reaches crisis level. In terms of cyber security, a crisis means a breach."

So, I'll ask again. How safe is your data? What kinds of cyber liability risks does your law firm have? What would you do if a member of your firm receives the Viagra e-mail and clicks on the link or opens the attachment? I will discuss these and similar issues in my next column.