CHICAGOLAWBULLETIN.COM

Serving Chicago's legal community for 160 years

MONDAY, OCTOBER 5, 2015

Chicago Daily Law Bulletin®

Volume 161, No. 194

Protecting law firm and client data

In my previous column (Aug. 3), I discussed how cyber liability is a serious risk-management issue for lawyers, given our Rule 1.6 duty to maintain the confidentiality of client information.

Given the high profile cyber-attacks against Target, Sony Pictures Entertainment, the U.S. government and the Ashley Madison website, many law firms may believe they are not big enough to be a target, or they don't have data that cyber-criminals would find attractive. These law firms would be wrong on both counts.

Even though they don't make headlines, law firms are increasingly becoming victims of cyber attacks because cyber criminals recognize that law firms are mostly unwilling or unable to take affirmative steps to protect the data they have.

This data would include things like client communications, client credit card transactions, client mailing and e-mail lists, patient health or medical records, employee payroll records, business and personal financial records, marketing plans and, of course, privileged legal, tax and financial communications.

One step a firm can take to protect client data is to read the end-user agreements for every vendor that has access to firm data. Firms who fail to read end-user agreements increase their risk of professional liability.

For example, you may be aware that Microsoft has released its newest operating system, Windows 10. They are generously allowing users to update for free for a limited time. How many of you reading this column updated to Windows 10 after reading the long and lengthy user agreement?

If you didn't read it, you missed a very important term that impacts your duty of confidentiality.

In a thoughtful and well-written LinkedIn post entitled "Windows 10 v. Rule 1.6," Ryan Johnson, co-owner of Torus Fiduciary IT, a management services provider in Phoenix whose primary focus is law firms, had this to say about the update:

"Apparently, Microsoft is following the footsteps of other 'Big Data' mining companies and has gotten creative in their user terms and conditions. How creative you ask, well apparently creative enough to give Microsoft ingress to virtually any and all data you may have or had access to while using their operating system!

"This ingress gives Microsoft permission to track your location, activities, browser history and more importantly, read your e-mails! Further, there does not appear to be a way for less sophisticated users to disable these settings. This is why it's so important to be aware of what's in that End User License Agreement."

The terms of the Microsoft agreement eliminate any expectation of privacy or confidentiality of client communications. Comment 17 to Rule 1.6 requires lawyers to "take reasonable precautions to prevent" the transmission of client communications to unintended recipients.

If you are unable to disable the settings as Johnson suggests can be done, you have willingly compromised the confidentiality of your client communications.

Another way law firms can protect themselves is to be aware of the kinds of data breaches that can and do occur.

Michael S. Flanagan is the co-founder and CEO of BigData Insure LLC here in Chicago that provides cyber insurance, solutions and services exclusively to law firms.

He explained that data beaches can occur when (1) a lawyer loses a laptop or smartphone that contains confidential client information; (2) the accounting department is tricked into sending funds to an unknown bank account; or (3) an e-mail is opened that infects malware into the system that is then used to corrupt files or to extort ransom for the return of your files.

If you want to gain some insight into the damage that can be caused from a data breach or a cyber-attack, look no further than the most recent attack on the Ashley Madison website; a dating website for married people.

First, the hackers threatened to expose all of the compromised data of some 37 million users unless the site was shut down. When the site was not shut down, the hackers dumped all of the data on the Internet.

While the embarrassment and humiliation of having your infidelity exposed would be damaging enough, the release of the contact and credit card information exposed users to identify theft and blackmail schemes.

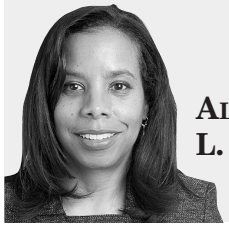
Just because we have yet to find a way to stop cyber-criminals, doesn't mean law firms should hold their hands up in resignation or defeat. There are at least four steps law firms can take to be more intentional in protecting firm data. The importance of reading all end-user agreements with all vendors who have access to client and firm data was discussed herein.

Law firms should also conduct a risk assessment of their firms and create and implement a cyber-security policy. All firms should review their insurance policies to see if coverage is included for a data breach.

It may be necessary to obtain cyber liability coverage because data is not considered a tangible property and it may be excluded from a general insurance policy.

And finally, the next time you receive a suspicious e-mail, just delete it.

WOODWISE ETHICS



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. Contact aw@legalethicsconsulting.com and follow her on Twitter at @WoodWiseEthics.