Wednesday, April 24, 2013

THE DAILY RECORD

WESTERN NEW YORK'S SOURCE FOR LAW, REAL ESTATE, FINANCE AND GENERAL INTELLIGENCE SINCE 1908

eDiscoveryUPDATE

Seven tips for better law firm security

\Today I will be in Las Vegas attending an electronic discovery conference. I was asked to not only attend the conference, but to speak on the topic of law firm security. What does law firm security have to do with electronic discovery you ask? Everything and then some.

Corporations allocate significant time and money for protecting their digital intellectual property. If you have ever met an information security professional, you know that they take their jobs seriously. Security is the reason the typical end user has to call IT every time they want to install an application. It is not job preservation; they are trying to protect the organization from malware, viruses and hackers, and sometimes the company's own employees.

By PETER COONS
Daily Record Columnist

So what happens when outside counsel shows up and wants to extract email from the archiving system because the company is being sued? Usually what happens is the lawyers get the email and the security guys are holding their breath.

Are they nervous? Is there any reason to be? Two weeks ago I was in California at a client location, let's call them CORP ABC. The week prior, outside counsel visited CORP ABC to collect emails and MS Office type documents in preparation for litigation. Clear instructions were provided to outside counsel that the collected data must be encrypted prior to shipment to D4 in Rochester.

When we received the data, we found it was not encrypted and the drive was marked CORP ABC Lawsuit. On the drive were thousands of confidential files, privileged emails, and a database that contained the "secret sauce." If this drive was lost or stolen, it would have been disastrous for all parties involved.

Once possession of that data was transferred from ABC to the law firm, they became the custodian of that data. I would argue that they had a professional and ethical obligation to protect it.

ABA Model Rule 1.1 states that "Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." ABA Model Rule 1.6 generally defines the duty of confidentiality and broadens that duty to "information relating to the representation of a client." This surely applies to digital information and the data collected from CORP ABC.

Additionally, Comment 16 to 1.6 reads:

"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.

In the example above, did the law firm comply with its ethical obligation to safeguard their client's data?

The scenario I outlined above is not extreme. Too often I see little thought or effort put towards protecting client data that is in the custody of law firms. Don't simply take my word for it. In late 2011, representatives from New York's top 200 were asked to meet with the FBI's cyber division in New York City.

The general message from the FBI was that hackers are targeting law firms to access data about their corporate clients and law firms are woefully unprepared to handle the onslaught. One security firm estimates that 80 major law firms were hacked last year. The general consensus is that law firms are soft targets.

Mary Galligan, who heads the FBI division that held the New York meeting, stated, "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." Right, why try to hack the bank when you can hack the banker's lawyers?

In Canada, seven law firms were hit in 2010 by Chinese-based hackers. The hackers were attempting to get the inside scoop of a $40 billion acquisition. One of the law firms involved identified the attack and they traced the intrusion to spyware that was installed after an employee opened a spoof email.

Seven tips to better security

1. If you are going to outsource any part of the legal process to

Continued ...

Reprinted with permission of The Daily Record ©*2013*

Wednesday, April 24, 2013

THE DAILY RECORD

WESTERN NEW YORK'S SOURCE FOR LAW, REAL ESTATE, FINANCE AND GENERAL INTELLIGENCE SINCE 1908

Continued ...

a third-party (e.g. e-discovery vendor), then vet that entity. Thoroughly investigate their security policies. Do they run background checks on their own employees? Where will the data be located? Insist on a site visit to verify what you are being told.

2. Talk to your IT staff at your company and get a handle on your network. At the FBI meeting discussed earlier, law firm representatives were told they need to diagram their networks and to know how computer logs are kept. "Some were really well prepared," Galligan said. "Others didn't know what we were talking about." Are there rogue access points or servers on the network that are not secure?

3. Make security a priority. If the managing partner at the firm isn't buying in to the security craze then you can bet no one below is either. Make it part of your company's culture. Many big law firms are touting their security prowess to attract bigger clients. So putting security at the top of the list can also have the benefit of getting (or holding) clients. Security makes good business sense!

4. Encryption is free. I love free stuff. You have to protect data that is on your laptop, iPhone, iPad, etc. You most likely have client data on one or multiple devices that you take outside the corporate firewall. When data is in transit it needs to be encrypted. There are plenty of free encryption tools out there so there is no excuse.

5. Education. This one could actually be 1 through 7. Educating your staff about security is probably the best way to keep data safe. Educate employees about spoof emails and why they should be deleted and not opened. You can have all the best security measures, but if people are not aware they are not worth a hill of beans. It is possible that in my CORP ABC scenario that the person that sent the data unencrypted had no idea what they were doing was wrong. Isn't there some saying about ignorance and the law?

6. Passwords. I know it is simple, but it's worth repeating. Use capital letters, symbols and numbers; don't use family names, pet names or birthdays. I saw a funny cartoon recently that had a picture of a dog with the caption, "… someone found out my password and now I have to get a new dog."

7. Don't use open Wi-Fi spots. This means when you are in Starbucks don't connect to the wifi on your iPad and start looking at client documents. If you travel a lot and need to access sensitive documents then talk to your IT staff about accessing those files securely.

One hundred percent security can never be achieved. The goal is not to be a soft target. Most hackers will move on to the next victim if they find your systems difficult to penetrate. Is your law firm doing all it can to safeguard client data?

Peter Coons is a senior vice president at D4, providing eDiscovery consulting services to clients. He is an EnCase Certified Examiner, an AccessData Certified Examiner, a Certified Computer Examiner (computer forensic certificates) and is a member of the High Technology Crime Investigation Association, the professional organization for people involved in computer forensics.

Reprinted with permission of The Daily Record ©*2013*