Data Breach Prevention and Due Diligence

Ellen Freedman, CLM

Lawyers are bound by ethical rules to safeguard client property, which includes confidential documents and other information. Just because your firm has anti-virus software and a firewall, and backs up faithfully every night, it doesn't mean your worries are over. There was a time when that would have been a sufficient standard to meet to protect yourself from possible disciplinary action, or a malpractice suit, in the event of a data breach. But the standard has continued to move upward, as the threat level has escalated.

It's really not a question of ***IF*** your firm will experience a data breach at some point, but rather ***WHEN*** your firm will experience the breach. Don't assume that your firm has no desirability as a target because of your size, or even your practice areas. Cyber criminals are increasingly targeting law firms of all sizes for private information about clients, which often enables them to more effectively target the client directly.

Eva Velasquez, President and CEO of the Identity Theft Resource Center says "While the overwhelmingly prevalent motive for data breaches remains financial gain for the thieves, we saw a shift in new motives for obtaining sensitive and private personal data this year. This compromised data can now be used to compel behavior changes in breached individuals and groups. This data is also being used for social justice purposes, and even to embarrass our nation."

One of the problems with understanding the severity of the problem is that data breaches often go unreported. So the problem is much larger than reported, despite the glaring headlines. In the legal industry, where maintaining client confidence is particularly essential, we hear only about the spectacular breaches.

In security circles, 2014 was regarded as the year of the credit card breach; 2015 is recognized as the year of the Social Security Number breach. Research shows 2015 almost doubled the 2014 tally of breached records in the first eight months alone. At this year's American Bar Association's TechShow, a complete track of courses focused on cybersecurity.

Glaring headlines in the March 29, 2016 The American Lawyer detailed that 48 of our nation's top law firms were specifically targeted by a Russian hacker seeking to trade on M&A information. Most of the firms found out they were a target only because their name was included in the article. On March 22, 2016 the FBI issued an alert warning law firms of criminals seeking access to their networks. Included in the FBI alert was this statement about recommendations: "Historically, industries targeted by cybercriminals have discovered that their networks were susceptible to intrusion due to lack of adherence to network security standards."

What should you do? First, realize that some of the largest firms have experienced breaches. And they have huge IT staff, and lots of money to throw at the problem. Don't throw up your arms in disdain and say you have no chance by comparison. For firms of all sizes I recommend you seriously consider the following measures:

1. **Test your system.** There are computer forensic experts who, for a modest fee, (based of course on the complexity and size of your infrastructure), will test your network to see what vulnerabilities exist, and give you a report and recommendations. If you deal with a small local IT vendor, don't assume they have the capability to properly secure your network. Use a third party expert to determine that. At one client, the IT company had reset the password on the firm's firewall router – which they should – but they used the number 123456 as the new password. PULEEZE!

2. **Encrypt.** Law firms have been extremely slow to adopt encryption. No, it isn't required by any current ethical opinion or rule. That doesn't mean you shouldn't do it. Especially on portable hard drives, laptops, tablets, etc. All data should be encrypted. The good news is that there is new software that does a great job even for email encryption. It's simple to use.

   By the way, if your system is breached but your hard drive is encrypted, it is not considered a breach which requires any notification.

3. **Password protect.** Make passwords required for everything, for laptops, tablets, smartphones, and anything that will take one. Use complex passwords that include alpha, numeric, and special characters. Use different passwords, not the same for everywhere, or a

"category" of places, like one password for all your social media accounts or travel accounts. To make this effortless, use a Password Keeper. I've been using LastPass for years. It will generate a new password upon request. More importantly, it holds all my current passwords securely in a vault on all my devices.

4. **Educate.** Research shows clearly that the largest vulnerability to exploit is human error. Opening an infected email, clicking on a phishing link, visiting an infected web site with no browser security, and other "should know better" behavior is still your greatest risk.

   There's much talk recently about the "gamification" of security education. In other words, having "fun" security drills to identify potential threats, with winners and prizes. One tends to ignore or forget the wagging finger in the face. But one rarely forgets something pleasurable and rewarding.

5. **Technology.** Keep all software patched for maximum security. Don't assume only certain applications count. For example, were you aware of the critical security update recently issued for Adobe Flash Player? (Which I can almost guarantee you have on your computer.) A security hole was found which enables takeover of your computer through a potential breach, which has already occurred in the wild. Likewise, you want to make sure the software for your firewall router(s) is up to date, and the password is secure. Hint: if you've changed IT companies, it is not secure. If your IT company is small, it is probably still the default "1111" password! Oh, and if you're still using Windows XP . . . I don't even have the words to properly describe your malfeasance.

6. **Monitor.** Probably one of the most astounding facts is that so many systems have been fully or partially breached, with the victim being clueless. Discuss with your IT vendor what you (or they) should be monitoring, so that you can detect a possible breach as quickly as possible. Often there are early warning signs at the beginning of certain kinds of breaches, and the breach can be shut down before real damage is done.

This isn't an exhaustive list, but I believe it includes the most important steps to take. As always, I include a reminder that I am here if you need additional assistance, vendor referrals, or just an understanding ear. Here's the bottom line: it's a dangerous computing world. We must work and live in it. You have to learn to navigate it safely, by rising to the current standard of due diligence.

A version of this article originally appeared in the
May 5, 2016 issue of PA Bar News

Freedman Consulting, Inc.
(215) 628-9422