The Deplorable State of Law Firm Information Security: Preventing Law Firm Data Breaches

by Sharon D. Nelson, Esq. and John W. Simek

Another day, another data breach. Data breaches have proliferated with amazing speed. In 2011, here was the roundup of some of the largest victims: Tricare, Nemours, Epsilon, WordPress, Sony, HB Gary, TripAdvisor, Citigroup, NASA, Lockheed Martin and RSA Security. Some mighty big names on that list.

Don’t be lulled into thinking that law firms (large and small) aren’t suffering data breaches just because they don’t have millions of clients affected. On November 1, 2009, the FBI issued an advisory warning law firms that they were specifically being targeted by hackers. Rob Lee, an information security specialist who investigates data breaches for the security company Mandiant, estimated that 10% of his time was spent in 2010 investigating law firm data breaches.

Matt Kesner, the CIO of Fenwick and West LLP, has lectured at ABA TECHSHOW and appeared on a podcast acknowledging that his law firm has been breached twice. As he has also noted, it is very unlikely that we know of most law firm data breaches since the firms have a deeply vested interest in keeping breaches quiet. This may be less true in the future now that 46 states have data breach notification laws. In fact, by the time you read this, it is possible that a federal data breach notification law will have finally been enacted – several bills were wending their way through the laborious legislative process in late 2011.

Shane Sims, a security practice director at PricewaterhouseCoopers has said, "Absolutely we've seen targeted attacks against law firms in the last 12 to 24 months because hackers, including state sponsors, are realizing there's economic intelligence in those networks especially related to business deals, mergers, and acquisitions.” Matt Kesner has noted that China is often responsible for state-sponsored hacking – and that China doesn’t waste its “A” squads on law firms because their security is so dreadful – the rookies on the “C” squads are good enough to penetrate most law firms.

While we agree, don’t be misled – garden variety cybercriminals are interested in law firm data as they engage in identity theft. This is as true for solos and small firms as it is for the big guys. Just think of the financial data that may be contained in the Separation Agreements drafted by family lawyers, almost all of whom are solos or in small firms. Those who practice the black arts of business espionage are also interested – and perhaps hired by the opposing party in litigation.

We hope we've piqued your interest in law firm data security and whether your own firm is secure. We wish there were a silver bullet for law firm security, but the truth is that there is no magical cloak to protect your data. You can be the first kid on your block to be infected with some sort of malware in what's known as a "zero day exploit" – meaning that you got the malware before the security companies have had a chance to muster a defense against it.

That said, there are some security basics that every lawyer should be aware of. Be very careful not to accept the word of your IT provider that you're secure. You need to do your own checking – or hire an independent third party to do so. There are legions of stories of IT providers who lawyers depended upon but who screwed up security and contributed to subsequent data breaches.

So away we go – our top practical security tips!

1. Have a strong password – at least 12 characters. No matter how strong an eight character password is, it can now be cracked in about two hours. A strong 12 character password takes roughly 17 years to crack. Much easier to hack someone else. Use a passphrase so you can remember the password: Love ABATECHSHOW 2012! Would be a perfect example.

2. Don't use the same password everywhere. If they crack you once, they've got you in other places too.

3. Change your passwords regularly. This will foil anyone who has gotten your password.

4. Do not have a file named "passwords" on your computer. And do not have your password on a sticky note under your keyboard or in your top right drawer (the two places we find them most often!)

5. Change the defaults. It doesn't matter if you are configuring a wireless router or installing a server operating system. In all cases, make sure you change any default values. The default user ID and passwords are well known for any software or hardware installation. Apple isn't immune either, since there are default values for their products as well.

6. Your laptop should be protected with whole disk encryption – no exceptions. Stolen and lost laptops are one of the leading causes of data breaches. Many of the newer

laptops have built-in whole disk encryption. To state the obvious, make sure you enable the encryption or your data won't be protected. Also, encryption may be used in conjunction with biometric access. As an example, our laptops require a fingerprint swipe at power on. Failure at that point leaves the computer hard drive fully encrypted.

7. Backup media is also a huge source of data leaks – it too should be encrypted. If you use an online backup service (which means you're storing your data in the cloud), make sure the data is encrypted in both transit and storage – and that employees of the backup vendor have no access to decrypt keys.

8. Thumb drives, which are easy to lose, should be encrypted – and you may want to log activity on USB ports. It is common for employees to lift data via a thumb drive – without logging, you cannot prove exactly what they copied.

9. Keep your server in a locked rack in a locked closet or room – physical security is essential.

10. Most smartphones write some amount of data to the phone – even opening a client document may write it to the phone whether or not you save it. The iPhone is particularly data rich. Make sure you have a PIN for your phone – this is a fundamental protection. Don't use "swiping" to protect your phone – thieves can discern the swipe the vast majority of time due to the oils from your fingers. Also make sure that you can wipe the data remotely if you lose your phone.

11. Solos and small firms should use a single integrated product to deal with spam, viruses and malware. For solos and small firms, we recommend using Kaspersky Internet Security 2012, which contains firewall, anti-virus, anti-spyware, rootkit detection, anti-spam and much more. For larger firms, we are fans of Trend Micro.

12. Wireless networks should be set up with the proper security. First and foremost, encryption should be enabled on the wireless device. Whether using Wired Equivalent Privacy (WEP) 128-bit or WPA encryption, make sure that all communications are secure. WEP is a weaker layer and can be cracked. The only wireless encryption standards that have not been cracked (yet) are WPA with the AES (Advanced Encryption Standard) or WPA2.

13. Make sure all critical patches are applied. This may be the job of your IT provider – too often, this is not done.

14. If software has gone out of support, its security may be in jeopardy – upgrade to a supported version to ensure that it is secure.

15. Control access – does your secretary need access to Quickbooks? Probably not – this is just another invitation to a breach.

16. If you terminate an employee, make sure you cut all possible access (including remote access) to your network immediately and kill their ID. Do not let the former employee have access to a computer to download personal files without a trusted escort.

17. Using cloud providers for software applications is fine **provided** that you made reasonable inquiry into their security. Read the terms of service carefully and check your state for an ethics opinions on this subject.

18. Be wary of social media applications which are now being invaded by cybercriminals. Giving another application access to your credentials for Facebook, as an example, could result in your account being hijacked. And even though Facebook now sends all hyperlinks through Websense first (a vast improvement), be wary of clicking on them.

19. Consider whether you need cyberinsurance to protect against the possible consequences of a breach. Most insurance policies do not cover the cost of investigating a breach, taking remedial steps or notifying those who are affected.

20. Have a social media and an incident response policy. Let your employees know how to use social media as safely as possible – and if an incident happens, it is helpful to have a plan of action in place.

21. Dispose of anything that holds data, including a digital copier, securely. For computers, you can use a free product like DBAN to securely wipe the data.

22. Make sure all computers require screen saver passwords and that it gets invoked within a reasonable period of inactivity.

23. Use wireless hot spots with great care. Do not enter any credit card information or login credentials prior to seeing the https: in the URL.

24. For remote access, use a VPN or other encrypted connection.

25. Do not give your user ID and password to anybody. This includes your secretary and even the IT support personnel.

None of these safeguards is hard to implement. Unfortunately, even if you implement them all, new dangers will arise tomorrow. The name of the game in information security is “constant vigilance.”

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and computer forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com