



LAWSITE

Texas Bar Today (texasbartoday.com) is a new State Bar website featuring news, insights, and commentary by Texas lawyers/bloggers. We update the site each weekday to feature and connect State Bar members. To add your blog to Texas Bar Today, email webmaster@texasbar.com.

WEBLINKS



LAURA McCLELLAN is a partner in the Dallas office of Thompson & Knight, L.L.P. She focuses her practice on real estate and real estate finance and blogs on commercial real estate topics (<http://relaw.typepad.com/real-estate-law-blog/>).

Evernote (evernote.com)

An amazing cloud storage solution that uses an online site and apps on my PC, Mac, iPhone, and iPad (also available for BlackBerry and Android platforms) to allow me to go virtually paperless in many areas of my life. Many more features than I can describe here, but this site is a game changer.

Dropbox (dropbox.com)

Another cloud storage solution that I use in a slightly different way from Evernote. Where Evernote is my virtual filing system, in Dropbox I save working documents (e.g., Word, Excel, PowerPoint) that I want to be able to access and work on from either my PC at the office or my Mac at home. No more emailing drafts to yourself so you can work on them remotely.

Lowering the Bar (loweringthebar.net)

A hilarious blog written by Kevin Underhill, who offers summaries and analysis of unusual and baffling legal escapades. Purely for entertainment, but worth dropping by for a laugh on a regular basis.



Preventing Law Firm Data Breaches

BY SHARON D. NELSON, ESQ. AND JOHN W. SIMEK
© 2011 SENSEI ENTERPRISES, INC.

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 Nov. 1, 2009, the FBI issued an advisory warning to law firms that they were specifically being targeted by hackers.

Matt Kesner, the CIO of Fenwick and West, L.L.P., 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.

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." 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.

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.



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.
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.
4. Do not have a file named "passwords" on your computer. And do not store 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. 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.
10. Have a PIN for your smartphone. 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. 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. 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.
15. Control access — 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. Giving another application access to your credentials for Facebook, as an example, could result in your account being hijacked.
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. 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 such as DBAN to securely wipe the data.
22. Make sure all computers require screen saver passwords and that the password 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 "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, including 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." ❖

SHARON D. NELSON, ESQ.

is president of Sensei Enterprises, Inc., a legal technology, information security, and computer forensics firm based in Fairfax, Va.

JOHN W. SIMEK

is vice president of Sensei Enterprises, Inc.