E-Security Pros Offer 15 Tips to Help Law Firms Better Protect Sensitive Data

By John W. Simek and Sharon D. Nelson

1. An eight-character password can be cracked in about two hours, while it takes over 100 years to reveal a strong 12-character password. Once you come up with a strong 12-character password, select a passphrase to help you remember it, don't share it with anyone — including your secretary or IT manager — and change it often.

2. Create different passwords for different uses so you aren't vulnerable across the board if one password is discerned. And don't store your passwords in a file named "passwords" on your computer, on a sticky note under your keyboard or in your top right drawer.

3. Change the defaults on your computers, whether you are configuring a wireless router or installing a server operating system. The default user ID and passwords are well known for any software or hardware installation, including Apple products.

4. Stolen and lost laptops are the leading causes of data breaches, so protect all laptops with whole disk encryption. Many newer models have built-in whole disk encryption, but you have to enable the encryption or your data won't be protected. Some encryption can be used in conjunction with biometric access.

5. Thumb drives, which are easy to lose, should be encrypted. You may want to log activity on USB ports, because it is common for employees to lift data via a thumb drive. Without logging, you cannot prove exactly what was copied.

6. Backup media, a huge source of data leaks, 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 transit and while being stored. Also, be sure that employees of the backup vendor do not have access to decrypt keys.

7. Keep your server in a locked rack in a locked closet or room. Physical security is essential.

8. 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.

9. 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 weaker 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.

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

11. 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 current ethics opinions on this subject.

12. Be wary of social media applications, as they are now frequently 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.

13. Consider whether you need cyber insurance 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.

14. 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. Also, remind employees to use wireless hot spots with great care.

15. 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.

John Simek and Sharon Nelson are president and vice president of Sensei Enterprises, a legal technology, information security and computer forensics firm based in Fairfax, Va. They can be reached at (703) 359-0700; jsimek@senseient.com *or* snelson@senseient.com.

Editor's note: Another version of the authors' e-Security recommendations can be found online at *www.americanbar.org/publications/law_practice_magazine/2012/january_february/hot-buttons.html.*