Managing the Security and Privacy of Data in a Law Office

By Dan Pinnington

Computers and the Internet have transformed the practice of law and how lawyers handle confidential client information. Where once paper documents were the norm, clients, lawyers, and law office staff now routinely work with electronic documents and data. Protecting the security and confidentiality of that information, however, is as important as ever.

Failure to take appropriate steps to protect electronic data in your office could have disastrous consequences, including an embarrassing release of sensitive information, malpractice claims, complaints to the Attorney Grievance Commission, or personal identity theft. At the very least, the theft, loss, or destruction of practice-related or client data will disrupt you and your practice. In extreme cases, it could cause your practice to fail.

To minimize the risk of any disclosure or loss of confidential client or practice data, you should understand where the risks are and implement office management practices and appropriate technology to ensure your data remains confidential and secure.

Following are various steps you should take to make sure the electronic information in your office remains confidential and secure. Although some of the suggested steps may not be relevant to every lawyer, all practitioners should find this information helpful. Even if you do not have the expertise to implement the suggested measures yourself, you'll be in a better position to direct the work that technology consultants or others must do for you.

An unprotected computer can be infected or hacked within seconds of connecting to the Internet, so safeguarding your electronic data is a must. The question is, how much time, effort, and money are you willing to invest in that task? Ultimately, you need to find a balance between the allowable risk and an acceptable cost and effort. From a best practices point of view, there are 13 steps you should take to protect the electronic data in your firm against the most common threats. Most can be completed quickly and at little or no cost.

(1) Install the latest updates to eliminate security vulnerabilities. The networking functionality built into software that allows the Internet to operate can create security vulnerabilities that, in turn, can allow computers to be compromised by hackers. Protect yourself by installing the latest security patches and updates.

(2) Make full and proper use of passwords. We all have more passwords than we can remember. As a result, we get lazy and use obvious passwords or none at all. You must use passwords, and use them properly, to keep your data safe.

(3) Antivirus software is essential. Computer viruses are a fact of life. Every computer in every law office should have antivirus software, and it needs to be configured to update automatically. Make sure you understand how to properly use and configure your antivirus software.

(4) Avoid spyware and malware. A virus isn't the only threat you have to worry about. There are several other malicious software threats, including some that will spy on you. Odds are they are already on your computer. You need to take steps to make sure no one is watching your surfing habits or collecting personal or client information from your computer.

(5) Install a firewall on your Internet connection. When you are connected to the Internet, the Internet is connected to you. Information flows freely both ways across your Internet connection. You need a firewall to act as a gatekeeper to prevent unauthorized access to your computers and network.

(6) Be aware of and avoid the dangers of e-mail. E-mail is an essential communications tool in most law offices,

An unprotected computer can be infected or hacked within seconds of connecting to the Internet, so safeguarding your electronic data is a must.

Law Practice Solutions is a regular feature brought to you by the Practice Management Resource Center (PMRC) of the State Bar of Michigan, featuring articles on practice management for lawyers and their staff. For more resources offered by the PMRC, visit our website at http://www.michbar.org/pmrc/content.cfm or call our Helpline at (800) 341-9715 to speak with JoAnn Hathaway or Diane Ebersole, Practice Management Advisors.

but it is also one of the most dangerous. E-mail is a common way that malware will enter your office, causing breaches of confidentiality and other serious problems. You and your staff must recognize the dangers of e-mail and know how to use it safely.

(7) Beware the dangers of metadata. Are you unwittingly sending confidential information to clients or opposing counsel? If you have emailed a Microsoft Word or other document in native format to clients or opposing counsel, the answer to this question is likely yes, and you need to learn more about metadata.

(8) Lock down and protect your data, wherever it is. Electronic client information is everywhere—inside your office on servers and desktop computers and outside your office in e-mails and on laptop computers, smartphones, and tablets. People can retrieve data across networks and even via the Internet. Understand who has access to your information and how to limit or prevent access to it.

(9) Harden your wireless connections. Connecting to the Internet with wireless technology is easy and seductive. However, if not configured properly, wireless connections can give hackers easy, unimpeded access to the data on your computer and network. Wireless users beware!

(10) Learn how to safely surf the web. The Internet browser is another dangerous tool in your office. Even casual web surfing can expose you to viruses and worms and divulge personal data. You and your staff need to know how to safely surf the web.

(11) Change key default settings. Every computer program and piece of hardware has certain preset or default settings necessary for them to operate out of the box. However, default settings are common knowledge, and hackers can use them to compromise a computer or network. You can make your systems much safer by changing some key default settings.

(12) Implement a technology-use policy. Law offices that use technology must understand basic dos and don'ts and where dangers lie. Every law office should have a basic technology-use policy that clearly informs staff what they can and can't do while e-mailing, surfing the web, and using other office systems.

(13) A backup can save your practice. You hope and pray it never happens, but even if you take all the above steps to reduce the likelihood of a malware infection or hacker attack, your system may be compromised. Nothing will be more valuable to you and your practice than a full backup of your critical practice and client data.

Don't be tempted to skip or skimp on one or more of the suggested steps. Remember, your data is only as safe as the weakest link in your security plan. When you leave for vacation, you lock every door and window in your house; leaving just one door or window open gives a thief easy and instant access. To make sure the security and privacy of your electronic information is properly protected, it is critical that you fully and properly implement all the above steps. ■

This is an excerpt from Managing the Security and Privacy of Electronic Data in a Law Office, *originally published by Lawyers' Professional Indemnity Company. It is reproduced with permission.*

Dan Pinnington is the vice president of claims prevention and stakeholder relations at the Lawyers' Professional Indemnity Company in Toronto (www.lawpro.ca) where he is the driving force behind practicePRO, LAWPRO's innovative and internationally recognized claims prevention initiative. Dan is a Fellow of the College of Law Practice Management and is a writer, speaker, and blogger on risk management, legal technology, and law practice management issues.