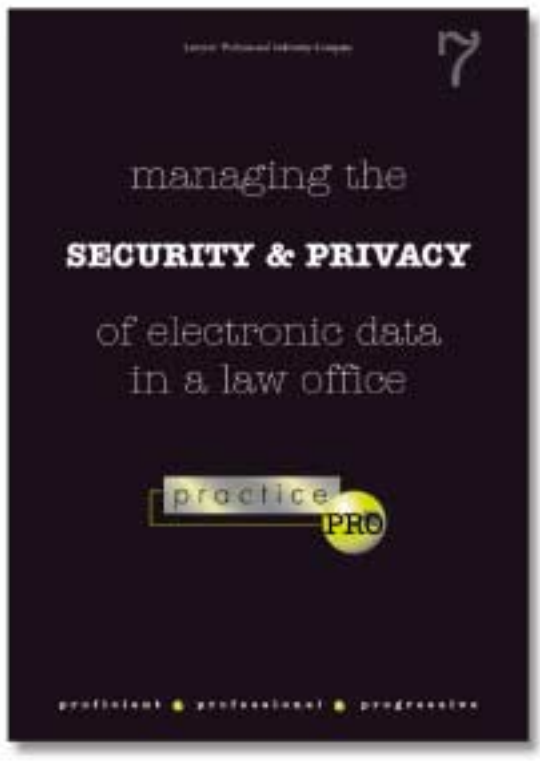
If you do nothing else –

the lucky 13

– things you must do



*(Ed note: The following is one of several checklists and tips available in **Managing the Security and Privacy of Electronic Data in a Law Office**, the seventh in a series of practice and risk management booklets from practicePRO. The booklet is now available in PDF format at www.practicepro.ca/securitybooklet. Copies will be mailed to all LawPRO insured lawyers in early 2005.*

From a best practices point of view, these thirteen steps are the minimum that you should take to protect the electronic data in your firm against the most common threats. Most can be completed very quickly, and at little or no cost.

1. **Install 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. Microsoft products are particularly vulnerable. 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, and as a result, we get lazy and use obvious ones, or don't use them at all. You must use passwords, and use them properly to keep your data safe.
3. **Antivirus software is essential:** Every computer in every law office should have antivirus software on it, and this software needs to be frequently updated, at least weekly. Make sure you understand how to properly use and configure your antivirus software.
4. **Avoid spyware and adware:** Once you had to worry only about viruses. Now there are several other malicious software threats that you need to be aware of, 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 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 can flow 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 – and one of the most dangerous. E-mail is one of the most common ways that viruses will enter your office, and can cause breaches of confidentiality and other problems. You and your staff must appreciate 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 e-mailed a Microsoft Word or Corel WordPerfect document to either, the answer to this question is likely yes, and you need to learn more about metadata.
8. **Lockdown your data, wherever it is:** Electronic client data is everywhere, both inside your office (on servers and desktop computers), and even outside your office (in e-mails, on laptop computers, cell phones, and PDA's). People can access data across networks, and even across the Internet. You need to understand who has access to your data, 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 can give hackers easy and 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 one of the more dangerous tools in your office. Even casual surfing on the Web 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 every piece of hardware has certain preset or default settings. These are necessary to make them 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:** Everyone using law office technology must understand basic do's and don'ts, and where the dangers are. Every law office should have a basic technology use policy that clearly informs all staff of what they can and can't do while using e-mail, surfing the Web, and using other law office systems.
13. **Make a full backup of your data:** If your system is ever 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 on 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 of the above steps. Working your way through the booklet ***Managing the Security and Privacy of Electronic Data in a Law Office*** will help you complete all the work necessary to protect the security and privacy of your data.