Lawyers' Professional Indemnity Company

7

managing the

SECURITY AND PRIVACY

of electronic data in a law office

practice PRO

proficient professional progressive

Proficient. Professional. Progressive

practicePRO® is the Lawyers' Professional Indemnity Company's innovative risk management initiative. It is designed to help lawyers adapt to the changing practice climate and to the opportunities that change presents.

Programs. Products. Processes.

practicePRO is a multi-faceted program of tools and resources to help you and your practice thrive.

Managing the security and privacy of electronic data in a law office is just one of several booklets in the practicePRO managing booklets series. Other practicePRO resources available to lawyers include: articles and information to assist lawyers in avoiding malpractice claims; "how to" practice aids that assist lawyers in efficient, effective and profitable practices; information on legal technology; education initiatives; and promotion of wellness and balance.

For more information on how you can put practicePRO to work for your practice see the last page of the book or contact practicePRO at 416-596-4623 or 1-800-410-1013

www.practicepro.ca

table of contents

© Lawyers' Professional Indemnity Company (LAWPRO)
1 Dundas Street West
Suite 2200
P.O. Box 75
Toronto, Ontario, Canada
M5G 1Z3
www.lawpro.ca

Disclaimer
This booklet includes techniques which are designed to minimize the likelihood of being sued for professional liability. The material presented does not establish, report, or create the standard of care for lawyers. The material is not a complete analysis of any of the topics covered, and readers should conduct their own appropriate legal research.

introduction

Computers and the Internet have transformed the practice of law, and how lawyers handle confidential client information. Where once paper documents were the norm, today clients, lawyers, and law office staff routinely work with electronic documents and data. Protecting the security and confidentiality of that information, however, is as important today as ever: Both the Rules of Professional Conduct and the Personal Information Protection and Electronic Documents Act (PIPEDA) apply equally to paper-based files and to electronic documents, such as a computer files or e-mail messages.

A failure to take appropriate steps to protect the electronic data in your office could have disastrous consequences. This could include an embarrassing release of sensitive information, a malpractice claim, a complaint to the Law Society, or the theft of your personal identity. At the very least, the theft, loss, or destruction of client or practice-related data will be disruptive to you and your practice. In the extreme case, 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 all of your data remains confidential and secure.

This booklet provides a comprehensive review of various steps you should take to ensure that 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 will find helpful information in this booklet. 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.

If you do nothing else – the lucky 13 things you must do

An unprotected computer can be infected or hacked within seconds of connecting to the Internet, so protecting 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 thirteen steps that you should systematically 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. More detail on each of these steps is provided in the remainder of this booklet.

#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. You must protect yourself by installing the latest security patches and updates. (See page 7)

#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 we don't use them at all. You must use passwords, and use them properly to keep your data safe. (See page 10)

#3 **Antivirus software is essential:** Computer viruses are a fact of life. 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. (See page 13)

#4 **Avoid spyware and adware:** Viruses used to be the only threat that you had to worry about. Now you need to be aware of 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. (See page 16)

#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. (See page 18)

#6 **Be aware of and avoid the dangers of e-mail:** E-mail is an essential communications tool in most law offices, but it is also one of the most dangerous tools. E-mail is one of the most common ways that viruses will enter your office, causing breaches of confidentiality and other serious problems. You and your staff must appreciate the dangers of e-mail, and know how to use it safely. (See page 19)

#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. (See page 23)

#8 **Lockdown and protect your data, wherever it is:** Electronic client data is everywhere, both inside your office (on servers and desktop computers), and outside your office (in e-mails, on laptop computers, cell phones, and PDAs). 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. (See page 28)

#9 **Harden your wireless connections:** Connecting to the Internet with wireless technology is so 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! (See page 35)

#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. (See page 37)

#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. (See page 41)

#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. (See page 43)

#13 **A backup can save your practice:** You hope and pray it never happens to you, and you will take all of the above steps to reduce the likelihood of a malware infection or hacker attack, but 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. (See page 45)

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 this booklet will help you complete all the work necessary to protect the security and privacy of your data.

Lastly, look inside your firm for potentially the most dangerous people, your own employees, and be especially careful of departing employees. (See page 48)

#1 install latest updates to eliminate security vulnerabilities

Computer software programs sold today are incredibly complex. Microsoft Windows XP, for example, has more than forty million lines of code written by thousands of programmers. Not surprisingly, programs often contain coding errors that were not detected prior to their release, and that can create problems, ranging from non-functioning features or functions to program lockups or crashes that result in data loss or file corruption.

These same coding errors can also cause security vulnerabilities that a hacker can exploit to access or destroy data, or run programs on a vulnerable computer, without the computer owner's knowledge. Once hackers become aware of a security vulnerability, they use tools to search the Web for computers that are open to attack.

To address these issues, software vendors make available updates or patches – usually as free downloads on the software vendor's Web site. They are also sometimes called service packs. You should regularly check that you have all the latest updates for all the programs on your computer.

Microsoft product users beware

Because Microsoft products are particularly prone to security vulnerabilities, you should update all Microsoft software regularly. Be aware if you are using any version of the Microsoft Windows operating system (Windows 98, Windows Me, Windows NT, Windows 2000 or Windows XP), Word, Excel, PowerPoint, Internet Explorer, Exchange Server, Outlook or Outlook Express.

- Updates to Microsoft Windows: Go to www.windowsupdate.com and follow the instructions. The tools on this Web page will review the Windows software on your computer (without sending information to Microsoft), and tell you what updates are available. Those that address security vulnerabilities are identified as *critical updates*. Other Windows and driver updates will also be listed. You don't have to install all available

updates, but you should work through and install all security-related updates. Some security updates must be installed individually, and most require that you restart your computer after they have been installed.

- Updates for Microsoft Office applications such as Word: Go to http://office.microsoft.com/ and follow the instructions.

Windows Automatic Update

Windows Automatic Update (formerly called Critical Update Notification) streamlines the updating process by notifying you when critical updates are available for your computer. Once activated, Automatic Update periodically checks with the Microsoft Web site for any critical updates for your system. It automatically downloads updates and notifies you when they need to be installed. All you do is wait for the installation prompt to appear and follow the on-screen instructions to complete the installation.

For greater control and automation, there are other products for managing the installation of updates from a central location.

Be careful with Windows XP Service Pack 2

Although Microsoft's Service Pack 2 update (SP2) for Windows XP contains some important security updates, users have reported problems with various programs and hardware operating properly afterwards. Before you install SP2, do some research to ensure it will not cause problems with the programs and hardware on your computer. For more information see www.microsoft.com/windowsxp/sp2/sp2_whattoknow.mspx.

Update all your software

If you are using non-Microsoft PC software, check for updates on the product's Web site. Sometimes direct links to an updates Web page can be found on the Help menu. Click on Help, then look for a link to a Web updates page. Otherwise, you should be able to find the product's site with a search on Google.

You are not immune to vulnerabilities if you use Linux or a Mac; these also need to be updated.

Backup before you install updates

Installing updates can interfere with the way a program works, or with the operation of the computer itself. Back up data on your computer before you install patches or updates. See page 45 for more information on backups.

#2 make full and proper use of passwords

We all have more passwords than we can easily remember, and as a result, we get lazy and use obvious passwords, or we don't use them at all. However, like the keys that open your front door or start your car, computer passwords "unlock" your computer. They are essential for properly securing and accessing electronic data so you need to be conscientious about how you set them up and use them.

How to properly use passwords

The following are steps you can take to use passwords more effectively:

- Never write down your password, especially on your monitor. Take a walk around your office and see how many passwords you can find on monitors.
- If you absolutely have to write down some of your passwords to remember them, don't write them out exactly. Write them out so they have to be translated in some way. For example, add or delete a character, transpose letters, or vary them in some other consistent way that only you can figure out.
- Don't tell anyone your passwords, ever. You are the only one who needs to know your passwords. Once someone else knows your password, you lose control over who can access your computer.
- Change any compromised password immediately. To be completely safe, you should change your passwords even if you only suspect they have been compromised.
- Don't use the same password for everything as this gives someone full and easy access to your entire system if they know that password. Try to use different passwords for different programs, especially for important or sensitive applications such as network logon or bank accounts.

- On Windows 2000 and XP computers, don't have identical passwords for your network logon and administrator account passwords.
- Change your network and other important passwords every 60 to 90 days. This will frustrate people who have your password without your knowledge.
- Be careful about where you save passwords on your computer. Too often users have a Word or WordPerfect file with all their passwords in it. This file can be located in seconds, especially if it is called password.doc, or if it contains the word "password." Consider getting a tool such as Password Manager XP (www.cp-lab.com) which will store your passwords on your computer in an encrypted and password-protected database.
- Be wary of dialog boxes, such as those for remote access and other telephone connections that let you save or remember your password. Do not select this option as it makes your password available to anyone who accesses your computer. Similarly, don't let your browser remember your Web site passwords.

Creating "strong" passwords

Create passwords that are harder to guess or figure out. These are called strong passwords and they are more difficult for password-cracking tools to determine. Password-cracking software uses one of three approaches: intelligent guessing, dictionary attacks, and automation. Automation is sometimes called brute force as it simply tries every possible combination of characters. Given enough time, the automated method can crack any password. However, it still can take months to crack a strong password.

For a password to be "strong", it should:

- Be at least eight characters long;
- Contain at least one character from each of the following four groups:
  - Uppercase letters A, B, C, ...;
  - Lowercase letters a, b, c, ...;
  - Numerals 0, 1, 2, 3, 4, 5, 6, 7, 8, 9; and
  - Symbols (all characters not defined as letters or numerals, including: ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /
- Have at least one symbol character in the second through sixth positions;
- Be significantly different from any passwords you have used previously;
- Not contain your name or your computer user name; and
- Not be a common word or name.

Treating passwords as confidential keys to your computer helps properly secure your firm and client data.

Antivirus software is essential to protect your computer and data from malware – the generic name for computer programs such as worms and viruses that are designed, as the name suggests, solely for malicious purposes.

Viruses

Like their biological namesakes, viruses are small programs that infect other programs on other computers, and in the process replicate and spread themselves further. Most viruses distribute themselves by e-mail, but they can also be spread by diskettes, and in many types of computer files, including Microsoft Word documents. Viruses bury themselves deep within the executable code in the programs they infect, making it difficult, if not impossible, to detect their presence, often after damage or data loss has occurred. There are tens of thousands of known viruses.

Worms

Worms are an even bigger threat because they replicate more easily than viruses. They embed themselves in e-mail messages or Web pages, lying dormant until the computer user opens an infected e-mail or accesses an infected Web page, at which time they will spread rapidly. Two of the more recent major worm incidents saw millions of computers across every continent infected in less than ten minutes.

Trojan Horses

Inspired by ancient Greek mythology, Trojan horse programs sneak malicious code onto your computer by hiding themselves within safe-looking programs, such as screen savers, games, titillating images, and other free downloads. Like other malware, Trojan horses can destroy your computer data or capture and share confidential information. See page 16 for more information on adware and spyware.

Antivirus software

Antivirus software effectively prevents virus and worm infections, although it may slow your computer down a bit. Once installed, the software continuously monitors other programs running on your computer. It will attempt to stop any virus activity it detects, hopefully in time to prevent further infections and data loss or damage.

The type of antivirus software you select depends on your computer. For computers that are not networked or are on a peer-to-peer network, use "personal" versions. Some corporate versions operate from a central server, others protect an e-mail server. No matter which type you select, antivirus software should be installed on all computers in your office — even those not connected to the Internet.

The two most widely used antivirus programs are Norton Antivirus (www.symantec.com) and VirusScan (www.mcafee.com). Expect to pay $40-$60 per computer to buy the software, plus an additional annual fee for virus signature file updates (see below). Buying antivirus software that is bundled with other products, such as firewall and anti-spam software, will save you money.

A free program that is a good option for a home computer is the AVG antivirus program from Grisoft (www.grisoft.com).

To scan a computer that doesn't have antivirus software on it, consider Housecall (www.trendmicro.com) and ActiveScan (www.pandasoftware.com/activescan).

Installing antivirus software however is only the start: You also need to regularly update your virus definition or signature files. Antivirus programs use the information in these files to recognize virus infections when they are occurring. As there are new viruses being created every day, you need to have the most recently released virus signature file to be protected against all possible infections. The updates to these files are available on your antivirus software's Web site. Expect to pay about $30-$40 per year for these updates, starting on the first anniversary of your installation.

Most antivirus software programs can be configured to download these updates automatically, without user intervention. Make sure the automatic update feature is enabled in your antivirus software as this ensures that your protection is always up-to-date.

Lastly, and most importantly, run your antivirus software to scan your entire hard disk(s) at least weekly, either manually or automatically.

Of far greater practical threat than any worms or viruses are adware and spyware – two new types of malware that likely have already infected your computers, unless you have taken specific steps to protect yourself and clean them from your systems.

Adware

Adware is software that tracks your surfing habits, and displays targeted pop-up advertisements on your computer based on Web sites visited or search terms used. *Pop-ups* are the advertisements that appear in separate browser windows while you are surfing the Web. In some cases, adware can also modify the settings on your computer. To protect yourself, you need to disable some types of Javascript and ActiveX controls in your browser. See page 37 for directions on how to do this.

Not all adware is illegal: The licensing agreements of some software programs allow the program to function as adware. Carefully read the licensing agreements of any program that you install on your computer, especially free screensavers and demo games.

Spyware

Spyware is software that surreptitiously installs itself on your computer, usually through dishonest means such as a Trojan horse or an unsolicited file download through your Web browser. Its function is to monitor and log system activity. Some spyware programs record every key a user types, then store that information on the hard drive of a computer. The spyware creator can then access and scan that information for passwords, bank account numbers, SIN numbers and other confidential information or client data. In other words, spyware makes your computer vulnerable to hacking, fraud and identity theft.

Recognizing and avoiding spyware and adware

Is your computer acting strangely? Is it running very slowly? Is there unexplained hard drive activity or Web traffic when you are not actively using it? Was your browser home page changed? If so, you may have a virus, spyware or other sort of malware on your computer. Adware and spyware can be extremely difficult to remove from a computer.

Because current antivirus software has only basic functionality to protect you from adware and spyware, you should use products specifically designed for this purpose. Two good products to consider are Ad-Aware (www.lavasoftusa.com) and Spybot S&D (http://security.kolla.de). They are easy to download and install, and should be used together as they will each catch things the other will miss. The free personal version of Ad-Aware may not be used on business computers.

For maximum protection, run Ad-aware and Spybot every week or two, and, update them regularly. Unfortunately, you'll have to check the products' Web sites regularly for updates, as they don't include an automatic update feature.

Regardless of whether you use a high-speed Internet connection, or dial-up modem, your systems must be protected by a firewall – a type of gatekeeper that ensures all incoming and outgoing communications are legitimate.

For computers to transmit data back and forth over the Internet, lines of communication must be established. These work through *ports* which are opened on each computer. The problem is that all the computers on the Internet can see one another, and these open ports can allow unauthorized people to access a computer. A firewall watches these ports and will warn you about or prevent unauthorized communications.

Firewalls come in two varieties: software and hardware. Software firewalls are easier to set up, usually protect a single computer, and are adequate for personal use. ZoneAlarm Pro (www.zonealarm.com) is a highly rated software firewall that is easy to install and use, and costs $70 per year. The more basic ZoneAlarm is free for personal use, and suitable for a home computer.

Hardware firewalls are usually used to protect an entire network of computers. D-link, Linksys, Netgear and others make relatively inexpensive hardware firewalls, which are suitable for a small office network, Cisco and others make firewalls for larger networks.

Windows XP's built-in firewall called the Internet Connection Firewall protects you only from incoming threats; it does not monitor or stop outgoing communications. XP users should consider a more robust hardware or software firewall. Note, you should disable the XP firewall if you use another firewall.

Probe your ports to test security vulnerabilities

ShieldsUP! (www.grc.com) is a free online program that scans your computer and its Internet connection looking for disclosure of personal information, open ports and other vulnerabilities. Within minutes, you'll know if your Internet connection has any security vulnerabilities.

#6 be aware of and avoid the dangers of e-mail

E-mail has become a vital tool in every law practice. Yet its widespread use exposes your firm to significant risks, including embarrassment, Law Society complaints, or malpractice claims due to the unintentional disclosure of confidential information, as well as data loss or destruction due to viruses or the downloading of other malware programs.

Firms should educate their staff on the dangers of e-mail, and have a clear, written policy on the proper use of e-mail. (See page 43 for information on technology use policies).

Password protected access

All e-mail programs can be configured to require a password at login. To prevent people from reading other peoples' e-mail, or from sending a message in someone else's name, make sure all e-mail account logins require a password.

Take care before hitting send

It's easy to inadvertently send an e-mail to the wrong person, potentially disclosing confidential or privileged information. The following steps can help you avoid making this mistake:

- Make sure each client's e-mail address book listing includes the client's full name. Using generic addresses such as Fred007@aol.com alone can create confusion.
- Make it an office policy to double-check that e-mail is addressed to the correct individual before it is sent.
- Educate your staff about the necessity of protecting confidential information, so they can recognize circumstances where information should be protected and not disclosed.

Privacy statements

Many firms include a privacy statement in their e-mail messages, often in the signature text at the end of a message. From a practical point of view, anyone who mistakenly gets the message will have read it before they read the privacy statement. For this reason, some question their real value, but most feel that having such statements are worthwhile. There is also some suggestion that you should only put privacy statements on messages that contain sensitive information as putting them on every message could lessen their credibility.

E-mail encryption

Theoretically, e-mails are easy to intercept, and as they are usually sent in an unencrypted format, they could be read by anyone who intercepts them. Practically speaking, intercepting an e-mail message is very difficult in most circumstances. The use of encryption software is not mandatory for all e-mail communications. However, the risk of interceptions and the options to encrypt messages should be discussed with any client you intend to e-mail. When information is extraordinarily sensitive, a lawyer should use, and advise the client to use, encryption software to help maintain confidentiality.

Unfortunately there are no universal standards for encryption of e-mail messages. Some e-mail programs can encrypt messages; as well, there are many different third party e-mail encryption programs. Verisign (www.verisign.com) and PGP Personal 8.0 (www.pgp.com) are among the more widely used. Others include FileAssurity (www.articsoft.com), SecExMail Personal (www.bytefusion.com), and CenturionMail 2.0 which integrates with Outlook (www.centurionsoft.com).

Web-based ZipLip (www.ziplip.com) and Hushmail (www.hushmail.com) offer on-the-fly message and file encryption. Both allow replies to be encrypted.

Don't be fooled by phishing

Did you know that e-mails appearing to come from companies you trust may actually be from criminals trying to steal your money or identity? So-called 'phishing' e-mails have quickly become one of the most devastating scams on the Internet.

Phishing scams use *spoofed* (faked or hoax) e-mails and Web sites to trick you into providing your personal and financial information. By using the trusted brands and logos of online retailers, banks, or credit card companies, phishing scammers trick surprising numbers of people. The phishing e-mail directs users to visit a Web site where they are asked to update personal information, such as passwords, and credit card, social insurance and bank account numbers.

Legitimate companies will not ask you to update your personal information via an e-mail message. Don't get tricked by phishing scams.

Spam filters

On a daily basis you undoubtedly receive unsolicited commercial e-mail, commonly know as *spam*. To combat spam, many firms use spam filters, which detect unsolicited and unwanted e-mail, and prevent those messages from getting into a user's inbox. Like other types of filtering programs, spam filters use various criteria to identify spam messages. Simple filters will watch for particular words in the subject line or sender's name, while more sophisticated filters attempt to identify spam through suspicious word patterns or word frequency. Anti-spam products also use *blacklists* which intercept messages from recognized spammers; and *whitelists* which let through messages only if they come from your personal list of recognized e-mail addresses.

Given that a significant proportion of spam messages also contain viruses or other malware, spam filters can also help protect your systems, and may prevent phishing scams from getting through.

While spam filters can significantly reduce the amount of spam you receive, they are not perfect. They will sometimes let spam through, and will sometimes block legitimate messages (these are called *false positives*). If you are using anti-spam software, you should scan blocked messages to ensure an important message wasn't missed. You also need to consider whether messages you send to others were intercepted by anti-spam software.

Anti-spam software can be installed on e-mail servers and/or on desktop computers. Some e-mail programs include anti-spam features. Popular third-party anti-spam products include Norton's antivirus software which includes anti-spam functionality (www.norton.com), SpamNet from Cloudmark (www.cloudmark.com), and Postini (www.postini.com).

E-mail savvy staff can help stop infections

Teaching your staff to avoid dangerous activities can also help reduce your exposure to potential infections. Employees should be taught to take great care in opening e-mail attachments, and not to open attachments that they are not expecting. Even if the message is from someone they know, they should not open it because it is easy to fake or spoof the sender's name. They should also be taught to take extreme care in downloading and running programs on their computers. Implementing a "no downloads rule" is the best protection.

#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. When you create and edit your Word or WordPerfect documents, information about you and the edits you make is automatically created and hidden within the document file. This information is called *metadata*. Metadata can be simply described as "data about data." Think of it as a hidden level of extra information that is automatically created and embedded in a computer file.

On its Web site, Microsoft indicates that the following metadata may be stored in documents created in all versions of Word, Excel and PowerPoint:

- your name and initials (or those of the person who created the file)
- your firm or organization name
- the name of your computer
- the name of the local hard drive or network server where you saved the document
- the name and type of the printer you printed the document on
- other file properties and summary information (see below)
- non-visible portions of embedded OLE objects
- the names of previous document authors
- document revisions, including deleted text that is no longer visible on the screen
- document versions
- information about any template used to create the file
- hidden text, and
- comments.

Similar (although less) metadata exists within WordPerfect files, and metadata data security issues affect the documents created in most other software programs.

While some metadata can easily be viewed within the program that has created a file, in most circumstances hidden metadata can only be seen with special software. However, hidden metadata can become visible accidentally – for example, when WordPerfect opens and improperly converts a Word file, or when a corrupted file is opened. In these instances, both of which are quite possible in a law office, the normally visible text and hidden metadata can appear on a computer screen.

The problem with metadata, especially for lawyers, arises when people electronically share files as an attachment via e-mail, on a floppy disk or CD-ROM, over a network, or through an extranet. Electronic document files include both the information you see on the screen, and all the metadata you don't see. This metadata can often be sensitive or confidential information, and can be potentially damaging or embarrassing if seen by the wrong eyes.

Metadata in Word

How can you view metadata in one of your Word documents? (WordPerfect users should jump ahead to "Metadata in WordPerfect," on page 25.) Find and open a letter or agreement that you recently e-mailed to a client or opposing counsel. Click on **File**, then **Properties**. This opens the **Properties** dialog box which contains a variety of summary type information about the file.

On the **General** tab you can see on which hard drive the document was stored, and the time and date it was created, last modified and viewed. On the **Summary** tab you can see the name of the author, your firm name, as well as the name of the template that was used to create the document.

The **Statistics** tab contains information about the size and structure of the document, including the **Total editing time** in minutes. This statistic is really the total amount of time the file was open on a computer, regardless of whether someone was editing it or not. What if a client saw this information, and the time indicated was significantly less than the amount of time you docketed for working on this document? This discrepancy could be completely justifiable, but you could find yourself explaining it to an upset client.

Metadata in WordPerfect

In WordPerfect you can see the basic file summary type of metadata you see in Microsoft Office documents by selecting **File**, then **Properties**.

WordPerfect also has a feature called Undo/Redo History. It can allow you to view hundreds of past changes in terms of what text was cut, copied and even deleted from the document. Open a WordPerfect document. Click on **Edit**, then **Undo/Redo**. This opens the **Undo/Redo History** dialog box which lists past changes to that document, assuming Undo/Redo is turned on. Click on the **Options** button, and then uncheck **Save Undo/Redo items with document** to turn it off. Look at some of your WordPerfect files to see if you can view summary metadata or the Undo/Redo History.

The danger of using existing documents as precedents

In many instances lawyers will adapt a document they created for a previous client. This makes perfect sense from an efficiency point of view. However, the text deleted from the original document can remain within the revised document. What would happen if your client sees confidential information about the client for whom the document was originally created, or if opposing counsel saw changes that were made in an agreement at the drafting or client review stage?

How do you remove metadata?

Being aware of metadata is just the start. You should also reduce or eliminate the metadata in your documents. Sending a fax or paper copy by regular mail would solve the problem, but will likely not be an option in many circumstances. If you want your client to review and edit a document, sending it electronically is the only practical option. In many cases, clients, opposing counsel and even the courts expect to receive documents electronically. There are a number of options to reduce or eliminate metadata from your documents.

Word, PowerPoint and Excel users should turn off the Fast Saves feature. To do this click on **Tools**, then **Options**, then the **Save** tab, and uncheck **Allow fast saves**. In older versions of Microsoft Office products it will be turned on by default. This feature lets a computer more quickly save a file by not removing deleted text.

If you use features such as tracked changes, document versions or comments, make sure you delete the information that is being kept within the document with these features.

Office XP includes some new features to help reduce the accidental disclosure of metadata. Even more features are included in Word 2003 and the other Office 2003 applications. They now include a Security tab in the Options dialog box (select **Tools**, then **Options** to view this tab). You can specify that some metadata not be saved in a document in this dialog box. The Information Rights Management feature in Office 2003 can also be used to reduce paper trail types of metadata being stored within documents.

Converting files to PDF format with Adobe Acrobat or other PDF creators will usually strip out most metadata. For this reason, many firms have adopted a practice of sending only locked PDF documents to clients or opposing counsel, especially if the recipient doesn't need to edit the document.

While converting a file to PDF format will help strip out metadata from the original document, remember that PDF files can also contain their own metadata. Select **File,** then **Document Properties** to view the summary metadata information within a PDF file. In this same dialog box you can add further restrictions on how the document can be accessed, used, copied and printed in the **Security Options** settings.

If you want the recipient to edit the document, send it in its native format, but without metadata. Several programs can help identify and clean metadata from your documents.

Microsoft's Remove Hidden Data Add-In permanently removes hidden and collaboration data, such as change tracking and comments, from Word, Excel, and PowerPoint files in Office XP and Office 2003 only.

For Word, Excel and PowerPoint documents, one of the most widely used metadata scrubbers is the Metadata Assistant, sold by Payne Consulting Group (www.payneconsulting.com) for US$79. Other metadata removal programs for the Microsoft suite of products include: Out-of-Sight (www.softwise.net); ezClean (www.kkl.com); Workshare Protect (www.workshare.net); and iScrub (www.esqinc.com), which integrates with Microsoft Outlook and will prompt a user to clean an outgoing attachment.

Unfortunately there is no software program that easily and automatically removes metadata from WordPerfect documents.

For more information on metadata, see the following resources:

- Word, Excel and PowerPoint users should visit the Microsoft support page at http://support.microsoft.com/. For more detailed information on removing metadata from Word 97, 2000 or 2002, see respectively, Knowledge Base articles 223790, 237361 or 290945.
- WordPerfect users should visit the Corel knowledge base at http://support.corel.com/ and search for "minimizing metadata."

Gone are the days when you had to worry about only one copy of each document, which you could easily secure by keeping it locked up in a file cabinet. Today, client data exists in electronic form in many different places inside and outside your office. You need to know where that data exists, who can access it, and what steps should be taken to secure and protect it.

Access to servers, routers and phone switches

Protecting your server and other key telecommunications equipment such as routers and phone switches starts with physical security. Intruders who have physical access to a server can get direct access to files and data on the server's hard drives, enabling them to extract usernames and passwords of every user on the system, destroy data, or give themselves a backdoor for accessing the server remotely. Even curious employees who want to change settings can unintentionally cause serious problems. Lock up your servers and other key telecommunications equipment to protect them from unauthorized access.

Access to individual computers

To protect information on them and on the network, every computer in a law office should be configured to require a password at startup. Without this password, it is more difficult to access the data on the hard drive. Although all versions of Windows accommodate this requirement, Windows 98 users should note that a login password will not protect data on a computer, as simply pressing the Esc key will bypass the login and give you full access to the hard drive.

Put a password on your screensaver

Activating a password-protected screensaver is a simple and very effective way to prevent an unauthorized user from rifling through the files of a computer that's been inadvertently left logged on. All versions of Windows include password-protected screensavers.

To activate this feature, click on **Start** and select **Settings** to open the **Control Panel**. Click on the **Display** icon, and select the **Screensaver** tab. Check the **Password protected** checkbox, enter a password, and set a **Wait time** that is appropriate for you. This is the amount of time the computer will wait after keyboard activity ceases before starting the screensaver. Once started, you require the password to exit the screensaver.

Access across a network

Anyone who has worked on a computer network will recognize that they have the ability to access computer files on another computer in the office, usually a central server. How does this work? The hard drive on a server contains various computer files and folders. To be seen and accessed across a network, folders and files on the server must be configured to be *shared*. To control access to files or folders (and all the files in them), the level of sharing and access can be limited, by either individual users or groups of users. Files and folders that are not shared can't be seen or accessed across a network. For example, you might give litigation staff *read-only* access to the folder with firm precedents so they can access them, but can't change them. You might limit access to folders with payroll information to your bookkeeper and managing partner. Client work product would go in a folder to which all staff had access.

The configuration of servers and networks will vary from office to office. Take time to understand what information is stored on your servers, and who has access to that information. Configure your network shares and access rights so that access to sensitive information is limited or prevented. Remember

that privacy legislation requires that you limit access to some types of personal information on a need-to-know basis.

Your desktop or laptop computer can act like a server in some cases, and content on your hard drive could be accessed by someone across a network, or from the Internet. To prevent this from happening you need to make sure that File and Printer Sharing is turned off on your computer.

Encryption of sensitive files

Many software products, including Word and WordPerfect, contain a feature that will let you password protect documents. Although this feature may prevent casual users from accessing password-protected documents, this type of password protection is easily circumvented. For files that contain extremely sensitive information, you may consider encryption. Encryption tools act as ciphers, converting information into secret code that can only be accessed with a password.

Windows 2000, NT, and XP have built-in functionality for encrypting files, but only on NTFS formatted hard drives. This offers some protection, although some software tools can decode NTFS-encrypted hard drives. Other file encryption products that are more effective than NTFS are listed in the next section.

Data on laptops and other portable devices

Laptops and personal data assistants (PDAs) contain large amounts of confidential client and personal information: They are also easily lost or stolen. As a first line of defence you can enable the built-in password protection on these devices. Although this should protect the data on them from the average thief, someone with specialized knowledge can bypass these built-in password-protection features.

For an extra level of security for laptops, consider using: PGP Personal 8.0 (www.pgp.com), PointSec for PC (www.pointsec.com); SafeGuard Easy (www.safeguardeasy.com); or SecureDoc (www.winmagic.com).

To encrypt the data on PDAs, the most widely used products include: PDADefense (www.pdadefense.com); PDASecure (www.trustdigital.com); PointSec for Palm (www.pointsec.com); SafeGuard PDA (www.safeguardeasy.com); or TealLock Corporate (www.tealpoint.com).

Never leave your laptop unattended in a public place. To be less of a target for theft, use a briefcase or bag that does not look like a standard laptop bag. Inexpensive cable locks from Targus (www.targus.com) and others may deter the casual thief, but are no obstacle for a determined thief with cable cutters.

E-mail encryption

E-mail messages carry confidential information outside your office and can, at least in theory, be intercepted. Encryption can prevent intercepted e-mail messages from being read, and is reviewed in more detail on page 20.

Deleted doesn't mean deleted

It's a misconception that deleted files are gone for good. In fact, deleted files are easy to recover using widely available forensic recovery tools. Even reformatting or repartitioning a hard drive will not completely destroy all the data on it.

This is an issue if you are sending your computer equipment outside the office for repair, or donating your computers to charity or a local school where a classroom of technology savvy students will be itching to recover your data.

To address this issue, you can use specialized software that will "scrub" all data from a hard drive so that it is not recoverable. WipeDrive (www.accessdata.com) is a widely used scrubber. Eraser 5.7 (www.heidi.ie), is a free download and is also a good scrubber. Physically destroying a hard drive with a hammer is the free and low-tech option.

Because the same forensic technology can also restore deleted files on floppy disks, you should always use new floppies when sending data outside your firm.

Remote access

Although a bonus for lawyers who want to work and access data when not in the office, remote access creates opportunities for breaches of confidentiality.

Virtual private networks or VPNs can make remote access more secure. A VPN is a network connection constructed by connecting computers together over the Internet and encrypting their communications so that intercepted data is incomprehensible. VPN's are secure and fast, but are expensive and hard to configure. Windows Terminal Server, which is free with Windows, will allow remote connections, is easy to set up, but is slower and less secure than a VPN.

Accessing your e-mail or network from a public computer

If you rely on Internet cafés, library terminals, or other public computers, be aware that you are likely leaving behind passwords, your surfing history, data in temporary files, cookies and other personal information at each machine you use. Products such as P.I. Protector Mobility Suite 2.0 (www.imaginelan.com) protect against this. The program, which you install on a USB flashdrive or other portable device, creates a portable identity on that device, including your e-mail data. The Protector program then accesses the Internet through the flashdrive or other device, and stores all sensitive information on it. As a result, you can use public computers without leaving a trace.

Be aware of data theft with thumbdrives

Tiny, high-capacity USB drives or thumbdrives have become the new floppies. A combination of three things makes them a security concern: (1) they are very easy to use, (2) they are compact, lightweight and ultra-portable, and (3) they can store huge amounts of information. They are, in other words, the perfect tool for a disgruntled or soon-to-be ex-employee who plans to easily and quickly steal firm data.

How do you protect yourself? Make sure you have appropriate security and access rights to the confidential client and firm information on your firm's computers and servers. Auditing file access may help you spot someone who is accessing information they should not. Consider disabling USB ports on all firm computers. Lastly, take extra care with employees who may be leaving the firm. (See page 48)

Off site storage

Storing electronic data with a third party raises a number of obligations to safeguard client property and confidentiality. These concerns also apply to data that is being backed up over the Web, or to matter documents that are being stored on a Web site for collaboration purposes.

Contracts with any third party who is in possession of confidential client information should deal with the various relevant securities issues, including having specific provisions that require all information is properly stored and secured to prevent inappropriate access. This can and should include password-controlled access and encryption of the information. In addition, antivirus software should be used. The third party should also indicate how the facility is prepared for a disaster, that adequate backup systems are in place, and what their contingency plans are if emergencies or disasters make the vendor's primary facility unavailable. These measures ensure that your clients' information is protected, and that you will have access to it when needed.

List serves and chat rooms

Through list serves, chat rooms and other virtual electronic communities, the Internet has created new ways to meet and mingle with others, including potential clients.

List serves, sometimes called e-mail lists, let you interact with dozens, hundreds or even thousands of other people. List serves are really nothing more than a group of people with the same address. You reach everyone on a list by sending an e-mail message to a specific e-mail address. List serve software operates by receiving this message, and then automatically sending it to everyone on the list. All replies are automatically sent to the entire list. In effect, this allows a large group conversation via e-mail.

Chat rooms are also called "online forums." Chat rooms are simply a page on a Web site or online service where people can "chat" with each other by typing messages on their computer. These messages are displayed almost instantly on the screens of others who are in that same "chat room." When you're in a chat room you can view all of the conversations taking place at once on your screen.

Saying something in a message posted to a list serve or in a chat room conversation is the same as blurting something in an elevator or at a meeting. All obligations of confidentiality still apply. Be aware of this and don't disclose confidential information on a list serve or in a chat room.

#9 Harden your wireless connections

Wireless connectivity is seductive, cool and offers endless exciting possibilities. You're no longer tied to your desk. You can take your laptop to a meeting down the hall and access local servers and the Web. At home or the office, you can easily connect multiple computers and printers, without running cables through walls and ceilings. You can stay connected in many public places, including coffee shops, restaurants, hotels, conference centers, and airport terminals. This is all possible because cheap, easy-to-use wireless technology has hit the mainstream.

Before you jump on the wireless bandwagon (and even if you already are a wireless user), you need to know that wireless is fraught with serious security issues. Installing a wireless device is like leaving the front door of your home or office open and unlocked. Anyone who can pick up your wireless signal could potentially access your Internet connection or data. Use wireless with caution, and only after you enable all possible security features on your wireless devices.

Why is wireless a security nightmare?

On the hardware side, wireless networking starts at a *wireless access point* or AP. The AP plugs into your wired network and has an antenna which broadcasts data via radio waves. These radio waves are transmitted to a receiver in a wireless *network interface card* (NIC) in your laptop or desktop computer, which in turn lets your computer communicate with the network without physically being plugged into it.

To make wireless products easy to use, they are generally shipped with all security features turned off. Although this makes installation a dream, it creates a security nightmare because it potentially allows anyone to connect to your network. So they are easy to locate and connect to, APs broadcast a *service set identifier* or SSID. This SSID is the name of your wireless network. The radio signal from your AP will radiate in a sphere 20 to 35 metres or more in diameter. Wireless-enabled laptops can scan their surroundings for SSIDs. Someone sitting in a car across from your home or office could easily

find and connect to your network. Hackers known as "wardrivers" actually cruise around looking for networks they can hack into.

Under older standards (802.11a, 802.11b and 802.11g), wireless device communications are not very secure. They allow easy interception of passwords and other information. A new standard, 802.11i, offers much stronger security, and devices compatible with it are now available.

For security reasons, many law firms will not install an AP on their networks. Firms that are installing wireless networks are using products such as the Aironet Series from CISCO. Although these products have more security features than the widely available consumer brand wireless products, they are much more expensive.

Wireless technologies will become even more common. If you are going to install a wireless network, make sure you get the newest wireless technology and enable all possible security features. Some generic directions for enabling security features on APs are available on our Web site at: www.practicepro.ca/securitybooklet.

Your Internet browser is 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, and how to configure your browser so that surfing is less dangerous. This involves disabling some browser features, controlling which cookies can be stored on your computer, and preventing pop-ups.

Locking down Internet Explorer

Malware programs can automatically install themselves while you are browsing or surfing on the Internet. These are called *drive-by downloads*. This can occur when Web sites run *scripts* (small bodies of code designed to perform a specific action) or *ActiveX Controls* (a module of code that adds extended functionality to the browser). You need to configure your browser so that it will warn you when this is happening, and stop it from happening, if necessary.

To do this for Internet Explorer versions 5.0 and later, click on **Tools**, then select **Internet Options**. Next, select the **Security** tab. Click on the **Internet** icon (the globe), and then click on the **Default Level** button to remove any custom settings.

Next, click the **Custom Level** button. This will open the **Securities Settings** dialog box. In the **ActiveX Controls And Plug-Ins** section of that box (at the top), configure the following settings as noted:

- Download Signed ActiveX Controls: Prompt
- Download Unsigned ActiveX Controls: Disable
- Initialize and Script ActiveX Controls Not Marked as Safe: Disable
- Run ActiveX Controls and Plug-Ins: Prompt
- Run ActiveX Controls Marked Safe for Scripting: Prompt

To save your changes, click **OK**, answer **Yes** to the **Are you sure you want to change the settings for this zone** questions, then click **Apply**, and **OK**.

After making these changes, whenever a Web site attempts to run a script or ActiveX Control, you will receive a prompt asking whether you want to allow that script or control to run. Click **Yes** if the message appears while you are visiting a reputable site. Click **No** if it appears when you are visiting an unfamiliar site.

Don't get eaten by the cookie monster

Spyware often works with the assistance of a *cookie*. Cookies are small files that provide a Web browser with information about a user such as identity information or preferences for visits to a particular site. One example would be your language preferences.

To protect yourself, you want to limit the types of cookies that can be stored on your computer. To do this, click on **Tools**, select **Internet Options**, and click the **Privacy** tab. By dragging the slider up or down, you can choose from six different levels of security, ranging from accepting all cookies, to total blockage of cookies, or various levels in between. To be safe, your setting should be at least Medium. This will protect you from third party cookies, which are the malicious type. Medium High or High settings provide greater protection, but may prevent some Web sites from running properly. To save your changes, click **Apply**, and then **OK**.

Preventing pop-ups

Pop-ups are the annoying windows that appear in separate browser windows while you are surfing the Web. Not only are they annoying, but they can also expose you to various types of malware. There are several software products that will intercept them and prevent them from loading. Pop-up Stopper (www.panicware.com) is very popular. Also widely used are the Google Toolbar (http://toolbar.google.com) and ZoneAlarm (www.zonealarm.com), which both include functionality for preventing pop-ups.

Instant Messaging can be insidious

At home and work, especially among younger people, *instant messaging* (IM) has become a popular form of online communication. IM is faster than e-mail and lets you communicate across the Internet with many people in real time. Although the features vary, at the core, most IM software products have two boxes for text in their main window. One box shows a running list of all comments from all participants in the conversation, the other box allows you to type your message. On pressing Enter, your message immediately jumps into the other box and goes out over the Web. IM products have little or no encryption or security, so IM statements are public and can expose your office to embarrassment. As well, IM makes it very easy to download or share files across the Web, and thus opens the doors for viruses, worms and other malicious code.

Many IM services are available for free on the Internet, including AOL Instant Messenger (AIM) (www.aim.com), ICQ (www.icq.com), and MSN Messenger (http://messenger.msn.ca). They are easily downloaded and installed, and they may already be running on your system.

IM can have a useful business purpose, but at present, it is usually used for personal conversations by office staff, often without permission. When using IM, it actually looks like staff are working hard on their computers. Most law offices will want to prohibit the use of IM in their technology use policy. (See page 43)

If IM is used in your office, be aware of it, and use antivirus, anti-spyware or firewalls to protect yourself from IM-related dangers. For further protection you should configure IM to hide personal information, turn off file sharing and receiving, and prevent downloads.

Disable messenger service

You can block pop-up spam messages in Windows NT, 2000, or XP by disabling the Windows Messenger service (this is unrelated to the MSN Messenger instant messaging program). Open the **Control Panel**, then click on **Administrative Tools**, and select **Services**. One of the running services will be **Messenger**. Right-click on it and select **Properties**. Set **Start-up Type** to **Disabled**, and press the **Stop** button.

#11 change key default settings

Changing the default values for hardware and software on your systems is another critical step in safeguarding the security of your data. This is the most technical of the thirteen steps outlined in this booklet[1].

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 the following key default settings:

- Administrator account name
- Domain name
- Workgroup name
- Outlook Web Access port

In the Windows world, the default administrator ID is *administrator*. Change the default name to something others won't know. Fortunately with the advent of Windows 2000 Server, there is no longer a default domain name. In Windows NT 4 Server, the default domain name is *domain*.

However, Microsoft has still held on to defining default workgroup names. The default workgroup name can be *WORKGROUP* or you may see *MSHOME* as the default. Workgroups are used to connect computers in a peer-to-peer environment. Change the default workgroup name to something less well-known, especially if you are in a shared office location and connected to other computers. All computers must have the same workgroup name to see each other and share files or resources.

To change or specify the workgroup for Windows XP, go to **Control Panel** and click on **System**. If you don't see System, then select **Performance and Maintenance** and then select **System**. Click on the **Computer Name** tab, and then click **Change**. Enter the desired workgroup name. Remember that this has to be done on all computers in your peer-to-peer network.

1 Adapted, with permission, from Security for Small and Mid-size Law Firms by Sharon D. Nelson, Esq. and John W. Simek, an article posted on Sensei Enterprises, Inc. Web site (www.senseient.com).

To change the workgroup in Windows 2000, go to **Control Panel**, and click on **System**. Click the **Network Identification** tab, and then select **Properties**. Enter the desired workgroup name in the workgroup box.

For Windows ME or 98, go to the **Control Panel** and then select the **Network** icon. Click on the **Identification** tab, and enter the desired name in the workgroup box.

If you are running an Exchange server or have installed Microsoft's Small Business Server, a few default values should be changed. Exchange allows remote access to a user's mailbox via a Web browser. *Outlook Web Access* (OWA) uses the default port 80, like most Web sites. This means that you have to allow port 80 to pass through your firewall to access your e-mail on the Exchange server. Unfortunately, port 80 is one of the most exploited ports by viruses and worms. The default port for OWA is the same as the default Web site on your Windows server. From the server, go to the **Administrator Tools**, and select the **Internet Services Manager**. Right click on the **Default Web site**, and select **Properties**. Change the **TCP Port value** to a value other than 80, and one that's easy for your employees to remember. The last four digits of a phone number is a good choice. Your firewall will have to be changed to allow the port that you configured for OWA. Assuming that you changed the port number to 9902, you access your e-mail by entering a URL in your browser that would be something like: http://mail.yourdomain.com:9902/exchange.

E-mail and the Internet have helped increase productivity in many law firms. But, as outlined in this booklet, they also expose a firm to significant risks. To address these risks, firms should: educate all lawyers and staff; and create a written policy that clearly establishes guidelines and minimum requirements governing the acceptable use of all firm technology resources.

A technology use policy should use simple and non-technical language that all employees can understand. It should be reviewed with new employees, and strictly enforced.

Every technology use policy should cover some basics. It should clearly state that technology resources provided by the firm, including Internet and e-mail access, are to be used for legitimate firm activities. Staff should understand that they have an obligation to use their resources properly and appropriately.

Technology use policies should also direct firm staff to ensure that confidentiality of firm and client information is protected at all times, that there is compliance with network system security mechanisms, and that resources are not used in a manner that would negatively affect others on the system.

Firms deal with personal use in different ways. Some firms allow occasional, reasonable use of Internet and e-mail resources, either on personal time, or even on company time. Other firms do not allow any personal use of these online resources.

Technology use policies should also indicate that the firm retains the right to monitor any and all electronic communications and use of the Internet to ensure the integrity of the firm's systems and compliance with the firm's technology use policy. As well, the policy should indicate that there may be sanctions for failure to comply.

The Law Society of British Columbia has a sample Internet and e-mail use policy for law firms on its Web site at www.lawsociety.bc.ca/services/Practice/body_practice_policy-internet.html.

Family computers are dangerous

Teenagers are more likely to engage in all the most dangerous activities, including using IM, downloading programs, and file sharing. If you use a compromised computer to log into your office, you can bypass the firewall and other security mechanisms and cause a security breach. Take the steps outlined in this booklet to protect your home computer. To be absolutely safe, avoid using a home computer for work purposes if it is used by others.

Another alternative is to have two partitions on your home computer. This essentially means there are two complete sets of software on the computer, one which only you would use, and one which others in the house would use.

#13 a backup can save your practice

Computers and other legal technologies have become critical to practising law. Every law firm has huge amounts of irreplaceable data on server and/or desktop hard drives. The most critical part of any disaster recovery plan is backing up the data on your firm's computers. A backup will allow you to recover when hard drives are infected by malware, if they are lost or damaged (due to theft or fire), or when they fail. Computer hard drives are complex pieces of electronic hardware that are subject to failure, and most ultimately will fail if they are used long enough.

To ensure you have a complete and reliable backup, follow these steps:

- Do a full backup: Full backups are better than partial backups. Having everything that was on your hard drive is better than finding out you need a critical file that wasn't backed up.
- Do backups daily: Modern backup hardware is able to do complete backups of large hard drives within hours. Backups can be set to run automatically, usually in the middle of the night. Doing a daily backup ensures you are as up-to-date as possible. It will have all of your work and data up until the end of the previous day.
- Identify responsible person(s) and alternatives: Doing the backup should be a mandatory responsibility that is assigned to a specific individual, and an alternate individual. You want to ensure that a backup is done every day, without fail.
- Review the backup log: Most backup software programs create a log report when a backup is completed. This report details what was backed up, and if there were any problems.
- Do regular test restores: Periodically, the backup log will report a successful backup when some or all of the data to be backed up was missed. The only way to truly test your backup is to regularly do a test restore of selected files and folders.

- Identify an offsite storage location: Tapes left on top of your server in your office could be destroyed or taken along with your server if there is a fire or theft. Don't keep all your eggs in one basket. You should store at least some or your backup tapes in one or more safe off-site locations.
- Rotate and keep generations of tapes: Don't use the same tape over and over; rotate your backup tapes. For example, use a series of five tapes, one for each night of the week. This can be helpful when database corruption is detected after it occurred. Having an older backup will allow you to reach back to an earlier date. Some firms keep end of week, end of month or end of year backups.
- Replace tapes regularly: Backup tapes degrade over time and with use. Replace them every six months. When tapes get to the end of their life, rotate them out as end-of-month tape etc.
- Don't forget data on other devices: Server backups usually are configured to only backup data on servers. Make sure that data on desktop computers, laptops and PDAs (Personal Digital Assistants) get backed up as well. Also, have staff back up the phone numbers stored in their cell phones.
- Make sure open files are being backed up: Some backup software will not back up files that are in use or "open" by other programs. Central accounting systems, e-mail and other database files often remain open 24 hours a day. Make sure that your backup is getting all open files.
- Create written instructions for restoring: Many offices have one or two people who know how to do a backup, but none who know how to restore backed up data. Create written instructions and train several people to do this task.

- Find a hardware backup buddy: If your backup server and tape unit are destroyed or stolen, you could find yourself with a good backup tape and no compatible tape unit to do a restore. Ideally find someone who has a server and tape unit that is identical to yours.

A full or partial backup from last week is better than no backup at all. If you are not doing full, regular backups, at least back up some of your most important files. It is easy to copy files onto a CD or some type of removable storage device. For a few hundred dollars you can purchase a small portable external hard drive with a very large storage capacity. Maxtor, Seagate and Western Digital are all reputable hard drive manufacturers. These are easy to plug into your computer via a USB port, and you can make a copy of all the data on a hard drive in a few hours or less. Some come with software that will back up an entire hard drive with one push of a button.

If you don't invest in any backup hardware, consider simply copying data to another computer on your network. This won't help if your office burns down, but it will help if you have a hard drive failure.

take care with current and departing employees

Most of us tend to look outside our offices for threats or dangers. However, you should also be aware of potential inside dangers. Statistics show that the majority of incidents involving the destruction or loss of data were perpetrated by current, soon-to-be dismissed or recently dismissed employees. Few, if any, know more about your firm's systems than your employees, and few, if any, are in a better position to cause major damage.

In particular, your IT staff, employees with advanced technology knowledge, and outside technology support people are potentially the greatest threat because they have the greatest knowledge about your system configurations, and the technical know-how to be very destructive.

When hiring a new employee, make sure you are diligent and carefully check their backgrounds and speak to references. Look for any red flags on an application letter or resume, and watch for issues during the interview process. Watch for someone that is withholding relevant information, or that has falsified information on the application. Assess the overall integrity and trustworthiness of the candidate.

When any employee leaves your firm, regardless of whether they are leaving of their own accord or are being terminated, ensure that your systems are protected. Promptly close all their points of access to your office and computer systems, including keys and access cards, login accounts and passwords, e-mail accounts or remote access. If you discharge an employee who has access to critical company data, let them go without notice, and don't allow them any access to a computer.

There are literally dozens of steps you should complete systematically to make sure all points of access for departed employees are closed down. A detailed departure checklist is available on the practicePRO Web site at www.practicepro.ca/securitybooklet.

Summary

LawPRO encourages you to proactively protect the security and privacy of the electronic information in your offices – not only to comply with the Rules of Professional Conduct and privacy legislation, but also to safeguard the viability and integrity of your practice.

A failure to protect the electronic data in your office could have disastrous consequences. This could include an embarrassing release of sensitive information, a malpractice claim, a complaint to the Law Society, or the theft of your personal or firm identity. At the very least, the theft, loss, or destruction of client- or practice-related data will be disruptive to both you and your practice. In the extreme case, it could cause your practice to fail.

Take time to understand where the risks are. Implement office management practices and appropriate technology to ensure all your data remains confidential and secure.

Carefully review and implement the suggestions and steps outlined in this booklet. Seek outside, knowledgeable help if necessary. It is relatively easy and inexpensive to protect yourself from the common threats. Acting now to protect yourself from the most common threats could help you avoid having to spend time and money dealing with security compromises.

Appendix 1 lists other resources that can help you secure the electronic data in your office.

Other resources

Web sites:

PC Magazine Security Watch page – www.pcmag.com/security
Various articles on security issues, and reviews of security related technology products.

Urban Legends Site Computer page – www.snopes.com/computer
An easy to use listing of current virus threats and hoaxes.

Symantec Home Page – www.symantec.com
Current information on the latest threats, list of known viruses, and information on how to repair and clean infected computers.

Consumer Web Watch – www.consumerwebwatch.org
A good page from *Consumer Reports* people for current news and information about Web-related security issues.

eBay Security and Resolution Centre – http://pages.ebay.ca/securitycentre/
Helpful information on avoiding online auction fraud and identity theft.

Senseient Publications Page – www.senseient.com
See the Publications Page for detailed articles on variety of law firm related security and forensics issues.

Test your password strength – www.securitystats.com/tools/password.php
Test the strength of your passwords, and get suggestions on how to make them stronger.

Tips For Troubleshooting Computer Problems – www.lawpro.ca/lawpro/Computer_troubleshooting.pdf
practicePRO article on steps to take to troubleshoot computer problems.

LSUC Practice Management Guidelines – www.lsuc.on.ca/services/pmg_tech.jsp
Guidelines to assist lawyers in conducting various aspects of legal work, including management of files and client information.

ABA's Law Practice Management Webzine – www.lawpracticetoday.org
General articles on legal technology and other LPM issues.

Office of Privacy Commissioner of Canada – www.privcom.gc.ca
Information on complying with PIPEDA.

Magazines

Smart Computing Magazine – www.smartcomputing.com
Great magazine for basic information on all types of technology.

Law Office Computing Magazine – www.lawofficecomputing.com
Great magazine for legal technology articles and product reviews.

Books

Computer Security for the Home and Small Office by Thomas C. Greene. Covers many of the topics covered in this booklet in more detail. 405 p. Apress, 2004.

Information Security: A Legal, Business, and Technical Handbook by Kimberly Kiefer, Stephen Wu, Ben Wilson and Randy Sabett; 82p. American Bar Association, 2003; www.ababooks.org.
This book reviews security threats, includes information on security best practices and how to respond to security incidents. It also has standards, guidelines and best practices precedents.

other tools and resources from practicePRO

practicePRO provides lawyers with a variety of tools and resources, in both print and electronic formats, designed to help your practice grow and thrive.

The "managing" series of booklets

These booklets provide insights and checklists to help lawyers better manage the risk associated with specific practice issues. Titles include: *managing the lawyer/client relationship*; *managing conflicts of interest*; *managing the practice of investing in clients*; *managing a mentoring relationship*; *managing practice interruptions*, and *managing the finances of your practice*.

The Online COACHING CENTRE (OCC)

The OCC is an online, self-coaching tool, comprising more than 150 modules, to help lawyers become more productive and effective in their professional and personal lives. Topics covered include: communicating powerfully; managing stress; overcoming procrastination; managing practice more efficiently; developing new business opportunities; and capitalizing on emotional intelligence.

Technology resources

practicePRO helps lawyers integrate technology into their practices through a variety of technology resources and articles.

Wellness resources

The practicePRO Web site provides links to assessment tools, guides and resources to help lawyers address wellness and balance issues.

Special Reports

Special Report on Litigation explores the increase in litigation claims, the forces driving change in litigation practice and the types of errors that underlie litigation claims, and provides practice management tips to help reduce exposure to claims.

Special Report on Fraud (Updated in 2004) examines real estate fraud, which increasingly targets lawyers, and provides tips to help lawyers recognize fraudulent transactions and how to avoid being a victim of fraud.

For more information on how you can put practicePRO to work for your practice contact us at 416-596-4623 or 1-800-410-1013 or see our Web site at www.practicepro.ca

About the Author:

This booklet was prepared for the Lawyers' Professional Indemnity Company (LAWPRO®) by Daniel E. Pinnington, Director, practicePRO, LAWPRO (dan.pinnington@lawpro.ca).

Lawyers' Professional Indemnity Company
One Dundas Street West
Suite 2200, P.O. Box 75
Toronto, Ontario M5G 1Z3

www.lawpro.ca