

Courting Disaster: Tools to Help You Create a Disaster Plan Now Security, Computer Backup, and “The Cloud”

Your office is your castle.....	2
Operating System	2
E-Mail Security.....	3
Encrypting Email	4
Spoofing and Phishing	5
Spear Phishing and Whaling.....	5
Spyware	6
Intrusion Detection Software (IDS)	7
Firewalls	8
Document Security.....	8
Sharing a Computer Network.....	9
Wireless LANs.....	9
Backup	10
Backup Hardware/Software.....	11
Online Backup	11
Cell Phone Security	11
Mobile Security	13
Encrypting Hardware	15
Laptop Security	15
Discarding Old Equipment	16
Social Networks and Security	16
Software as a Service	17
The Cost of Free	18
Resources from Dan Pinnington at practicePRO:	19

By Catherine Sanders Reach Director, ABA Legal Technology Resource Center

Your office is your castle

Like a medieval castle, your office is your fortress. Multiple walls are needed to keep intruders out, and additional precautions are needed to protect the King from internal dangers. In fact, some studies show that more techno-dangers come from within a business than from the outside.

What follows is an overview: detailing all possible threats and the possible protective steps to counter them is beyond the scope of this paper. Instead, it will focus on threats we believe you are most likely to encounter and common sense solutions that you can take to protect yourself and your data from falling victim to current security threats.

Information security does not have a one product, one-size-fits-all solution: Hackers and other criminals target some high-profile firms, because of the nature of their work, while others firms go unnoticed. Some firms may have a VPN, while another does not.

Each firm must implement appropriate security solutions while remaining vigilant to new dangers. Your reputation and success rest upon this vigilance. Protecting your computer and data is truly an instance where you are better to be proactive, to “go on the offensive” to take steps to safeguard yourself, your firm and your clients. So man the walls, raise the drawbridge and prepare for battle because the enemy is at the gate intent on pillaging what you hold dear!

Operating System

The first place to start in protecting yourself and your data, is by keeping your Operating System (“OS”) up to date. Microsoft Windows is the most widely used OS and is therefore the primary target for HACKERS and CRACKERS. No protection plan that you undertake will survive contact with the Cyber-Barbarians if you fail to keep your OS up to date. If you use Mac OS X or Linux, you’re not out of the cross hairs: vulnerabilities have been found in both of these and as they become more widely used, the number of attempted exploits will also increase.

Updates

Windows XP provides for several different options for automatic updates which can be activated as follows:

Click Start > Control Panel >Performance and Maintenance >System >Automatic Updates:

▶ This method will work if using the Category View for folders.

or

Click Start > Control Panel >System >Automatic Updates.

▶ This method will work if you are using Windows Classic view for folders. Make sure that the “Keep my computer up to date” checkbox is marked. Then select from one of the three options for downloading and installing updates.

▶ The first two options allow you to control and requires you to be involved in installation of each update. The third option will automatically download and install updates on the schedule you establish, thereby automating this process.

► Microsoft now publishes security updates on the Second Tuesday of every month.

You can also manually scan your system and download updates by accessing the Windows Update website at:

<http://v4.windowsupdate.microsoft.com/en/default.asp>

or

□

Click Start > Help and Support > Keep your computer up-to-date with Windows Update.

► This will take you to the Windows Update website which you can allow to scan your system for updates.

► Critical Updates and Service Packs are those updates that affect security and vulnerabilities of your computer – these should be downloaded. Windows Updates may include helpful updates, but also updates that you may not want, so review these before downloading. Driver Updates affect device drivers for your system and you should review these and consider them carefully before downloading.

E-Mail Security

Anti-virus protection is essential for every computer in a law firm or lawyer's home office. The first line of defense is to have an Internet usage policy for the office or firm. Require all lawyers and staff to only open email attachments from reputable sources. Do not allow non-work related attachments to be opened.

Just having the software is not enough. You must download the latest antivirus definitions to ensure the software contains the most up-to-date detection and prevention. Commercial anti-virus software publishers often sell update subscriptions for about \$30 per computer per year; enterprise licenses are much cheaper per seat.

Encryption is not required under the confidentiality rules in most states; however many leave it up to the lawyer to decide. If the information you intend to put in the email is so sensitive that you would not send it by courier or mail, then it probably needs to be encrypted. Also discuss the matter with your client; if they want it encrypted, then do it. There are commercial encryption products available, including on-line services. Work with your client to find the best solution for sending and receiving encrypted email.

Misaddressed emails can also breach attorney-client confidentiality. Like a fax sent to a wrong phone number, an errant email can do as much damage. In Microsoft's Outlook consider turning off the address "AutoComplete" function to avoid mistakes; remind staff to always double-check the addressee in each outgoing email. Finally, while I know of no authority that disclaimers in the email work, it still seems like a good idea. Try adding it above the message, rather than at the end, this will serve as a warning to any unintended reader.

Clearing spam filters becomes more important each day. Spam filters prevent our Inboxes from overloading, but spam filters are not fool-proof. Some spam gets through, while some important messages do not. Be sure to open your "Suspected Spam" folder on a daily basis to make sure nothing important was filtered out by mistake.

Retaining client emails is becoming more of an issue. Is an email message more like a letter or a phone call? If it is a letter, doesn't it belong in the client's file? If not, shouldn't it be discarded? Check your state's legal ethics opinions for more guidance in this area.

Email messages can be a ticking time bomb, and should therefore be treated with great care. Your firm should have a written policy addressing proper use of firm email for business communication by lawyers and support staff; storage and retention of email as a record; security issues including opening attachments, identifying spam and phishing, and other scams; use of firm email for personal communication; and use of other Internet based communication tools such as instant messaging, blogging, commenting on blogs, social networking, and online chat.

Encrypting Email

Confidentiality is the bedrock of the attorney-client relationship. However, this privilege is at risk during the routine transmission of an electronic communication. Email encryption reduces this risk. Email encryption obscures the content of the email in order to prevent people other than the sender and the receptor from reading the content. Additionally some encryption programs will provide proof that the document was received and disable the forwarding option so that the message cannot be forwarded. Increased availability and affordability make encryption an accessible option for safeguarding attorney/client privilege.

Encryption is not required under the confidentiality rules in most states; however many leave it up to the lawyer to decide. If the information you intend to put in the email is so sensitive that you would not send it by courier or mail, then it probably needs to be encrypted. Also discuss the matter with your client; if they want it encrypted, then do it. There are commercial encryption products available, including on-line services. Work with your client to find the best solution for sending and receiving encrypted email.

Email encryption vendors are responding to the marketplace and have begun to offer easy to use solutions for people who send and receive sensitive correspondence. These programs are designed to be simple for the user to implement and do not require additional hardware. While the recipient will be aware that an encryption program has been used, and they may need to be supplied with a password, they will not need any special software to access the email. The vendors understand that not all information needs to be encrypted so they offer flexibility to choose which messages are important to secure and track. As always, if a trial version is offered by the vendor, try before you buy to see if the program fits your needs.

[Dialawg](#) – This solution integrates with several email programs (Outlook, Thunderbird, Gmail) and mobile devices. It allows the user to send an email to the recipient, however the recipient receives a link, rather than the email itself. The recipient follows the link, logs in and reads the encrypted communication. The communication thread is all online, so the messages are not stored on anyone's computer. The transmission is encrypted as well (of course). The pricing is by matter, and recipients are never charged.

[SecuRmail](#) (from Rpost) – This email encryption solution claims to avoid storage of email in a web-based repository and encryption keys, as well as HIPAA compliance. The system basically automates the process of sending an encrypted PDF of the email that the end user wants to be encrypted. It works bi-directionally so the entire conversation remains encrypted. The password is sent via email too, automatically and in a separate file.

[Hushmail](#) - A standalone web based email encryption program. The user signs up for a free Hushmail account which allows them to send secured emails. For a fee, users can upgrade to a premium account which would allow them to send attachments. Hushmail is working on a plug-in for Outlook but at this time it was still in BETA mode.

See also:

[PGP Desktop Email](#) - A desktop e-mail encryption software program. The PGP Corporation makes encryption software for small/home office, small business, and enterprise customers

[PGP Corporation Product Comparison Chart](#) - A chart that compares different encryption products made by the PGP Corporation.

[EchoWorx Secure Mail](#) - Send client negotiations, contracts financials, and litigation via email securely

[IronPort PostX Secure Email](#) - A desktop e-mail encryption program

[Encrypt messages in Microsoft Outlook 2003](#)

[Encrypted messages in Microsoft Outlook 2007](#)

[How to Protect E-Mail From Prying Eyes](#)

(A PC World article explaining how to utilize e-mail encryption in Microsoft Outlook and Thunderbird, using free digital security certificates provided by [Thawte](#) or [Comodo](#))

Spoofing and Phishing

Central to many online identity theft schemes is a social engineering technique called “spoofing,” in which identity thieves create fake e-mails and websites disguised to look as if they originate from trusted sources. In “phishing” schemes, identity thieves use spoofed e-mails, websites and popups to “lure” users into divulging sensitive personal information such as usernames, passwords, credit card numbers, and social security numbers.

A typical phishing email might be designed to look as if it originates from a financial institution or an e-commerce company such as e-Bay or PayPal. The e-mail might ask the recipient to log into the bank or company’s website to verify account information for some spurious reason, such as that unusual account activity has been detected and that the account will be closed unless the user logs in and verifies their account details.

The e-mail would typically include a convenient link to click on that would take the user to a website masquerading as the bank or company’s website, complete with the bank or company’s logo and other details designed make the website look authentic. If the user were to enter any personal information into the fake website, such as usernames, passwords, and other valuable personal information, the website would record this information for later exploitation by identity thieves.

The phishers are getting smarter as surely as consumers get more wary. In one notorious phishing scheme occurring in August of 2007, the contact information of more than a million Monster.com subscribers was stolen and used in phishing e-mails. Identity thieves used a virus disguised as a job-search tool, which stole Monster.com users’ contact information after being downloaded. Users reported later receiving legitimate-looking email messages containing personal information such as their names, and which extended job offers with one catch--the job seekers would need to have Bank of America bank accounts in order to accept the offer. The emails included a link to a site that looked like a Bank of America website where they could allegedly open an account. When users entered their personal information into the fake Bank of America site, the site recorded the information for later use by identity thieves.

Spear Phishing and Whaling

Spear phishing and whaling are phishing schemes in which identity thieves carefully target and research their victims. Some companies post information such as company news, organizational structure, and employee biographies on their websites. Identity thieves can study and use such contextual information to target specific employees and make phishing e-mails seem more

authentic, such as making e-mails appear to originate from a trustworthy source within an organization such as a coworker or the organization's HR department.

A specific type of spear phishing is called whaling, in which identity thieves gather information in order to target an organization's executives in the hopes of gaining access to valuable trade secrets and other executive-level information that might result in a high payoff to the identity thieves. Examples include emails sent to executives purporting to be from the Better Business Bureau, or a question about an invoice, or a recruitment company. For a busy executive (or lawyer) who forwards the email on to the accountant or assistant to provide a response with the requested information this could be a surprisingly effective means of attack.

Spyware

There are many products that will remove adware and spyware from your computer; however, your first line of defense is your web browser. Which browser you use can have a lot to do with how much time you spend clearing your computer of malware on a regular basis.

Anyone who is even vaguely knowledgeable about the Internet knows that Microsoft Windows and Internet Explorer are both full of security holes and are very subject to viruses and malicious attacks. Even if you have hardware and software firewalls between your computer and the Internet and keep your virus software scrupulously up to date you are subject to the plague of pop-up and pop-under ads, and the ghoulies they may contain, which some web sites – even reputable ones, throw at you.

To make Internet Explorer safer to use, consider disabling the ActiveX controls. This can easily be done, but it does reduce the functionality of IE. Some IE users object to this, but many find no appreciable difference in their web browsing experience. It may be better to be safe than sorry.

Dan Pinnington, in his guide *Managing the Security and Privacy of Electronic Data in the Law Office*, suggests the following settings: 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 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.

Another secure alternative is not to use Internet Explorer, but a more secure competitor: Firefox.

Firefox is the free browser from Mozilla, the non-profit web development offshoot of Netscape. They have worked to produce a new browser to compete with Internet Explorer, and to clear up some of the problems Microsoft either can't, or won't, fix. It's a winner, as evidenced by the fact that it's already captured 15% of the worldwide browser market.

The browser has a nice, clean, simple look, which is very easy to modify. It comes set up with the requisite buttons for forward and back, stop, reload and home, and it's easy to go into the preferences and drag dividers, printer buttons, a little clock to show your browsing history, and other useful buttons onto the toolbar. For those who are used to using a Google toolbar on their

browser, it even comes with a little window you can use to do a Google search without even having to call up Google.

Getting the browser is easy. Just go to <http://www.mozilla.com/>, download it, and double click on the downloaded file to install. It will even ask you if you'd like to import your bookmarks from Internet Explorer!

Once you have a more secure browser, it's time to look at some anti-spyware products to sweep and clean up your computer. The chances are very good that, even if you haven't experienced the slowdowns and crashes that are the alarm-bell that malware is present, you have some of it on your computer.

The job of a good anti-spyware program is twofold: first it should locate and remove malware already resident on your computer; then, it should block new programs from downloading themselves in real time. Fortunately, you have many products from which to choose, and some of them are pretty good.

According to product reviews in recent issues of PC Magazine and PC World, one of the most effective malware detector/removers is Spy Sweeper from Webroot Software, Inc. – www.webroot.com. At only \$30 for a one-year subscription to the version that will also block malware before it has a chance to load, you can't afford not to have Spy Sweeper on your computer.

Counterspy from Sunbelt Software is also getting stellar reviews from the computer press, and at \$20 is a real bargain.

Ad-Aware from Lavasoft (www.lavasoftusa.com) is another well-known and fairly effective program, which comes in both free and fee-based versions.

There are two paid versions of the software: Ad-aware SE Plus and Ad-aware Professional. Ad-aware SE Plus includes all the features of the personal edition along with enhanced features such as real-time monitoring that allow you to delete malware before it infects your system. Ad-aware SE Plus for business or home use runs about \$40. The Professional edition contains additional features which allow you to analyze running processes, and costs about \$50. The Lavasoft site also offers a shareware registry editor called Reghance™.

While these spyware removal tools are great, the next generation of protection prevents the malware and spyware from loading onto your computer at all. These products for your web browser act like anti-virus software for e-mail. SpywareGuard and SpywareBlaster are two such products. These freeware products from Javacool Software help keep the bad stuff out, but as with many of these new programs, there may be compatibility issues.

The bottom line: None of the currently existing anti-spyware programs will stop or remove everything that the evil goblins that lurk hidden in the Internet can throw at your computer. Existing programs are constantly being updated, and new programs to combat new threats are constantly being developed. A combination of two or more programs, free and fee, is needed to give your computer the greatest possible protections.

Intrusion Detection Software (IDS)

Intrusion detection software fills the gaps between firewalls, anti-spyware, and anti-virus software. Hackers, spyware purveyors, and on-line criminals know where these gaps in protection exist, and are working hard to exploit them. IDS stops trojans, worms, hijackers, and other malicious

programs from getting in to your computer, but also prevents them from executing once inside your firewall. Again, no solution is perfect, but this new type of security software is important to own.

[Prevx Pro](http://www.prevx.com/) (<http://www.prevx.com/>) is one such product from Prevx Ltd. Another is [WinPatrol](http://www.winpatrol.com/) (<http://www.winpatrol.com/>), which also receives high marks in the software press. Symantec's (<http://www.symantec.com/>) small business solutions also promise intrusion prevention and Untangle's (<http://www.untangle.com>) open source Network Gateway also provides intrusion prevention.

Firewalls

According to the Wikipedia, a firewall is a piece of *hardware* or *software* that functions in a networked environment to prevent some communications forbidden by the security policy, analogous to the function of firewalls in building construction. It has the basic task of controlling traffic between different zones of trust. Typical zones of trust include the Internet (a zone with no trust) and an internal network (a zone with high trust). The ultimate goal is to provide controlled connectivity between zones of differing trust levels through the enforcement of a security policy and connectivity model based on the least privilege principle.

Typically, small businesses have used software solutions to control unwanted access to network and internet connected computers. These solutions include a basic firewall in Windows XP and Vista, Zone Alarm (www.zonealarm.com), Comodo (www.comodo.com), Kerio (www.kerio.com) and various versions from Symantec, McAfee, Trend Micro, Grisoft and others.

Larger enterprises often use firewall appliances from companies such as SonicWall, Barracuda Networks and WatchGuard—integrated hardware solutions to stop unwanted hackers and others. However, some of these appliances are now being targeted at smaller businesses; small to medium size law firms should consider this as a possible alternative to software alone.

There are also a number of free or open source products, including Untangle's Network Gateway which is free for the standard product and provides a firewall as well as anti-virus, anti-intrusion detection, site filtering and more, as well as Comodo (www.comodo.com) and Kerio (www.kerio.com).

Document Security

Documents are the lifeblood of attorneys. They contain the work product of the firm. Many lawyers share electronic documents with clients, co-counsel, opposing counsel and the courts via email, e-filing, and extranets. These documents more often than not contain sensitive client information. Lawyers have a duty to preserve the confidentiality of that information. Electronic documents, unprotected, can be copied, printed, edited, and reused by others.

One step law firms can take to protect sensitive information is to use password security on electronic documents. Microsoft and Corel office suites offer the ability to password protect documents. In MS Word 2003 under "Tools" "Protect Documents" you can limit editing to read-only, comments, and track changes. Under "Tools" "Options" "Security" you can enable password protection to open or modify a document. There are also privacy options, such as "make hidden markup visible when opening or saving" and "warn before printing, saving, or sending a file that contains tracked changes or comments". Similar options are available under the "Prepare" option in the Office Button of MS Word 2007, You may consider some of these security options within the firm when they make sense to protect client information or the integrity of the document.

Another way to protect documents from unwanted changes or exposure is to consider publishing to PDF. Using Adobe Acrobat or other PDF writing program, you can convert word processing files to PDF before sharing them. In Adobe Acrobat users can “lock down” documents, disallowing printing, copying, editing, commenting or even opening the document. You can encrypt the file or use secure digital signatures and authentication protocols. Attorneys can make sure that the document is used in the way they want, without exposing it to alteration or copying.

Sharing a Computer Network

Office sharing offers great opportunities to the solo practitioner or small firm. Not only can you cut real estate and personnel costs by sharing an office suite and clerical staff, but you have someone else around to bounce ideas off. And there lies the rub: when you’re not really part of a firm, you can’t ethically share some of these ideas.

The same is true of sharing office technology resources. In the last few years more and more lawyers have sought to cut costs by making their unused space available to other practitioners, and often the inducements to those practitioners have included shared technology resources such as phone systems and computer networks including fast Internet access. However, just as there can be ethical problems involving confidentiality issues and safekeeping of data with shared office space, there can also be potential problems with shared computer resources.

Do not leave your desktop computer unattended when it is on and you are logged in. Enable the password protection, and set it to override the system when it has been inactive for three minutes or less.

Biometric devices, such as thumbprint readers that authenticate the user may sound a bit geeky today, but with the prices falling to under \$100, expect to see more of this soon.

Log off the network if you are going to be gone longer than an hour.

Use a minimum of twelve digit passwords with a combination of numbers and letters—including alternate capitalization of the letters.

Confirm with the law firm network administrator that the network is configured to prevent unauthorized access to your computer. Get this in writing if possible.

Wireless LANs

Wireless networking can save a firm the time and expense of running cable to all parts on an office. However, wireless connectivity is neither as reliable nor as fast as wired networks. Yes, it is a close call and getting better, but there are plenty of safety concerns as well.

A wireless router or access point throws a signal about 100 feet, although the signal strength diminishes as it passes through walls. Firms can use this to reach place within the office not previously wired for computers. However, here is where the security concerns come in: Any person with a wireless access card (network card or wireless adaptor) can use your network, and potentially have access to your computer files and documents. The firm must take steps to secure the wireless network from prying eyes. Manufacturers build this security into all routers and access points, but the user must enable it. Whether the security protocol is WEP, WPA, or MAC addresses, make sure you secure the network against intruders.

One final point about wireless office network security: You may find that despite all the best advice and intentions, the network settings and security create too many conflicts and issues. The network may just be too unreliable. In the end, it may be more cost-effective just to run cable and be done with it.

Be sure to secure your home office wireless network too. While not as likely a target, there still may be neighbors who may hijack your network. Many lawyers who successfully install a wireless network are frustrated with security matters. New utilities are just coming to market that makes securing a wireless network a much less frustrating process.

If you are going to use a wireless network, you need to consider the following:

Enable ENCRYPTION available for wireless networks. Ideally, you want to use Wi-Fi Protected Access 2("WPA2"):

Rename the Service Set Identifier ("SSID"): Every wireless Router/Access Point has an SSID which is set at a factory default when initially setup. This is what differentiates one wireless network from another and is sent in plain text. To make it more difficult for someone to identify your wireless network you need to change the standard SSID and Administrator Password of your Router/Access Point.

Disable SSID broadcast if possible: If possible, you should disable the SSID broadcast.

Limit Number of Computers: If you only have x number of computers which will attach to the wireless network, you should limit the number of machines that can access the network to that number. As long as those computers are connected to the wireless network, no other machines can attach.

Router/Access Point Placement: Since the Router/Access Point generally broadcasts in all directions. Place the access point in the center of your building/office/home if possible - the closer to an outside wall that you place it, the further the range that someone can pick-up a signal.

Select infrastructure mode: You can select from 2 wireless modes – ad hoc and infrastructure. ad hoc mode allows wireless equipped computers to communicate directly with each other without the need of first communicating with a Router/Access Point. infrastructure mode requires each wireless equipped computer to use of the Router/Access Point to communicate.

Limit access by specific Media Access Control ("MAC") address: Each network card is identified by a unique MAC address. By limiting access to the wireless network by MAC address, even if one computer isn't attached, no one else can communicate with the Router/Access Point since their MAC Address will not be approved for access.

Consider disabling DHCP and assigning static IP addresses: This allows you to control which network addresses are assigned and which ones will be recognized by your Router/Access Point.

Backup

There is nothing more important in your office procedures than the regular back-up information stored on your computer. Back up means to copy your important computer files (such as client documents, software applications, time and billing data, and e-mail) onto another computer or media that can be accessed to restore data if you computer crashes, the file is corrupted, or your office is damaged or destroyed.

There are four components to a good back-up system: Automatic back-up software, a large and reliable local storage device, an off-site recipient storage device, and a competent person to make sure it runs correctly.

Backup Hardware/Software

Numerous software options are available and often come bundled with the storage device. Forget the old disc and tape devices, and go to external hard drives like Maxtor or ABS. The software is more important than the hardware, because it has to work well for the user or the user won't use it! Too often lawyers buy the back-up device but fail to use it because the software is cumbersome or does not have automatic settings. Consider Backup Now, BackupMyPC, Retrospect Backup, CMS' Bounce Back, or full image back-up software such as Norton Ghost (www.symantec.com), Acronis TrueImage (www.acronis.com) or Second Copy 2000 (www.secondcopy.com). Whichever method you choose, your office computer should be backed up daily. That is where the competent person comes in! Unless the backup system is used, the technology is worthless. Make sure a competent person carries out this important security step in your firm. Also, do a periodic test to restore a file to make sure your backup system is working.

Online Backup

With the growing availability of broadband internet access, online storage for your critical data is also an option. Ranging from products from Mozy (www.mozy.com) and Carbonite (www.carbonite.com) to offerings from Iron Mountain (www.ironmountain.com), iBackup (www.ibackup.com), these companies provide a wide range of support and services.

In ABA [Opinion 95-398](#) (10/95) (membership access required) the authors recognized that "in this era of rapidly developing technology, lawyers frequently use outside agencies for numerous functions such as accounting, data processing, photocopying, computer servicing, storage and paper disposal and that lawyers retaining such outside service providers are required to make reasonable efforts to prevent unauthorized disclosures of client information ." The outside service providers would be considered to be non-lawyer assistants under [Model Rule 5.3](#) which states that lawyers have an obligation to ensure that the conduct of the non lawyer employees they employ, retain or become associated with is compatible with the professional obligations of the lawyer. [North Dakota](#) is the only state thus far that directly addresses the ethical issue of utilizing online service providers. Other states refer to computer systems, third party access, and remote servers or file storage.

Lawyers should ensure that the right questions are asked and answered to make a reasonable attempt to protect the firm's data. Courtney Kennaday, SC Bar Practice Management Advisor, has posted a helpful list of questions to ask of online backup providers (<http://www.scbars.org/pmap/>) . This list can also help remind firms of questions to ask of *any* online service.

Cell Phone Security

The current generation of wireless communication gadgets is truly amazing, especially when you compare them with their "bag phone" ancestors of only a decade or so ago. You can sort through your contacts, schedule items on your calendar, read and send email, surf the Internet, read and

edit documents, listen to the radio or pre-recorded music, take and send photos, and talk to friends and clients, all on the same pocket-sized device.

Wireless communication tools break down into two basic types, based on their feature sets. They are:

Handhelds – Handhelds are the descendants of the personal digital assistant. They typically have an operating system, some pre-installed software, and allow you to download and install other programs, primarily through a cable or cradle, although they may also use an infrared interface, Bluetooth and/or, in the case of wireless handhelds, a connection to a wireless LAN. They are sometimes referred to as “wearable” computers.

Smartphones – Smartphones are the offspring of the marriage of the PDA and the cell phone. They look much like handhelds, but they pack the added punch of allowing you to send and receive calls. Although they may also be capable of synchronizing data with your workstation through a cable, they primarily rely on their wireless connectivity and your cell phone company’s network for information transfer.

In order to understand the current and potential security threats to these tiny life savers, you need to think about their status as “wearable computers” and how they came to be.

The development of the PDA and the convergence of the PDA and the cell phone parallel the development of personal and laptop computers in many ways. Just as computers started out with small operating systems and ran very few simple programs, so did PDAs. The desire for more programs on the PDA encouraged the development of larger and more robust operating systems, which in turn encouraged more robust PDA programs. Finally, owners got tired of having to enter calendar items, contacts and phone numbers into both devices, or having to sync their phones with their PDAs through various means, and the smartphone was born. And along with this convenience came plenty of the same security problems that computer users currently face.

First, because they are small and portable, handhelds and smartphones are infinitely subject to being lost or stolen, placing the information stored on them at risk. If the risk of the information becoming public is great enough, it simply shouldn’t be placed on any device which can be removed from the office in a casual manner. Otherwise, the device should be password protected and, if appropriate, the contents should be encrypted.

Second, these devices are slowly, but surely, becoming subject to all of the ghoulies and ghosties that personal computers encountered when they began to be regularly and consistently connected to the Internet, namely: viruses, worms, and Trojan horses.

As the virus writers get better, the possibilities for mischief, such as denial of service attacks and transmission of malicious code through handhelds and cell phones to other networked resources will increase. There is also evidence that cell phone virus writers are starting to work on pests for the Microsoft smartphone operating system.

As their operating systems and features become larger and more complex in order to accommodate consumer needs (or what the cell phone companies tell us we need), every added line of operating system code will become a potential source of additional security problems. And as more lawyers upgrade to more complex cell phone/PDA hybrids, their security worries will only increase.

A couple of current, and slightly more pressing, problems for some cell phone users are “bluejacking” and “bluesnarfing.” These are problems peculiar to Bluetooth® enabled devices.

For the couple of people left in the world who haven’t heard, Bluetooth is a relatively new technology which allows the creation of a PAN (personal area network between two or more

connected devices) using radio waves in the 2.4GHz range. Unlike infrared, Bluetooth does not require a clear line of sight and can connect within a standard range of about 30 feet, leaving open the possibility for great convenience in connecting electronic devices quickly and conveniently without wires, as well as the possibility for fun and games – or trouble. Bluejacking fits into the former category, and bluesnarfing into the latter.

Bluejacking is the act of creating a message in the form of a contact with your Bluetooth-enabled phone, and then shooting it to an unsuspecting person within range. As a form of high art, bluejacking messages should usually include a snarky remark about the person's phone or attire. Then you sit and snicker as the unsuspecting victim looks all around trying to figure out where the message came from, and why. Lawyers are generally pretty thick-skinned, and don't risk much damage from bluejacking, which doesn't appear to be illegal unless the communications continue to the point of becoming harassing. If you want to know more about bluejacking, go to www.bluejackq.com, the website of a very precocious British teen who goes by the nom-de-web of jellyellie. Bluesnarfing is another matter.

Bluesnarfing takes place when someone armed with a computer loaded with special software and, often, a directional antenna that can extend the range of Bluetooth, sets up shop in a prime location, waiting for unsuspecting folks to come along and tarry for a while, so that he or she can suck the contents out of the unsuspecting target's Bluetooth-enabled cell phone, including calendar items, contacts and any multi-media items, such as pictures, associated with them and, in some cases, even the IMEI (International Mobile Equipment Identity) – the phone's identifying information. Depending on the amount of information in the phone, the process can take as little as thirty seconds or as much as three or four minutes.

There are a number of encryption options for mobile phones. See [FYI: Security on the Go](#). According to the [2009 ABA Legal Technology Survey Report: Mobile Lawyers](#) more than four-fifths of respondents report using a smartphone while away from the office (82%, compared with 67% in the 2008 survey and 53% in the 2007 survey). The most regularly used feature was real-time e-mail (86%, compared with 75% in the 2008 survey and 68% in the 2007 survey). When asked what type of security was used to protect confidential information on a smartphone most asserted the use of password protection (90%), however only 6% reported the use of remote data wiping. Consider that in the city of Chicago alone the results of an [international survey conducted by PointSec Mobile \(now CheckPoint\)](#) reported that 21,000 "PDAs and Pocket PCs" were found in the back of Chicago cabs over a 6 month period. The good news? Almost 14,000 of these devices were reunited with their owners.

How does a cabbie find out to whom to return the lost device? Probably by turning on the device. If it is password protected they will have little luck. You could put a small sticker on the back of the device with a phone number to report the phone if it is found. However, another safety net is to install or deploy the ability to remotely wipe the device if it should become lost or stolen. [PC Magazine has an article that describes methods and software to remotely wipe smartphones](#) including BlackBerryOS, iPhone, AndroidOS, PalmPre and Windows Mobile devices. Consider remote wiping as an extra step to keep your client's confidential information out of the hands of others.

The bottom line: How much connectivity do I really need in my practice? Is having a way to capture information while I'm away from the office, and then sync it with my computer when I return a sufficient tradeoff for increased security?

Mobile Security

Many firms are now using notebook computers as full-time replacements for desktops PCs. Lawyers can take them to and from court, depositions, home, etc. Other lawyers are using

smartphones or PDAs to store data while on the road. However, this mobility also increases security risks.

Portable devices have a bad habit of being lost, stolen or misplaced. The loss of the computing device is bad enough, but the loss of client data is far worse. All firms must take steps to prevent unauthorized access to client data. All devices must be password protected. Furthermore, if the inadvertent disclosure of client data on your computer would be harmful or embarrassing, then be sure to use encryption technology for all client documents and data.

Mobile security issues also include remote access to your office network from authorized users. The number of lawyers and staff who choose to work outside the office has exploded! We now want to work when we want to work, from home, beach houses, and vacation destinations around the world. The technological tools are many; each firm must choose the remote tools that work best for their circumstances. However, with such flexibility comes a variety of security issues.

Remote access can take a variety of favors, but all involve Internet connectivity in one way or another. Many small firms use Internet subscription services like GoToMyPC to access their office computer from any Internet-connected computer. Others use software such as PCAnywhere to access their office computer from home. Still others use more robust (and expensive) tools such as a Microsoft Exchange server or a Citrix server. A full discussion of these options is beyond the scope of this paper; security remains our focus.

Whatever your remote access tool you use, institute the following policies:

All access must be password protected; all passwords to change every 60-90 days; no partner or employee of the firm may disclose his or her password to anyone. This includes prohibiting any user from using the "Remember me" feature (that automatically completes login names and passwords) on their remote computer. This is especially true for employees who use the family computer at home.

Require all remote users to have the same level of Internet security as the law firm: Any computer seeking to access your network must use firewalls, anti-virus software, anti-spyware, etc.

Review the security policies regularly to make sure system integrity is maintained.

If you do not need frequent remote connectivity, try a USB flash drive instead of a remote access system. A USB Flash Drive memory unit is a revolutionary way to transport and share files. This tiny device is smaller than a marking pen yet can hold up to 1G or more information-client documents, presentations, photos, or music. Just plug and play into the USB port on any computer! It is the perfect tool for transporting files between home and office. Try the Lexar USB JumpDrive Traveler—a flashdrive with extra software so that you can use a public computer and not leave a trace of information behind. For example, you need to check email and edit a document during your vacation in Disney World. Just plug in your JumpDrive Traveler and all your emails and document tracks are saved to the flashdrive, not the host computer. So you can carry documents and work on them confidentially without lugging a computer with you.

If you are going to use mobile computing then follow these recommendations:

Use a Software Firewall.

Consider using encryption for your e-mail and digital signatures.

Disable your wireless cards ad-hoc option.

Disable file and printer sharing.

Disable your wireless card if you're not working online.

Be aware of anyone looking "over your shoulder" as you enter your passwords.

Consider using VPN software and a VPN endpoint if you have them.

Don't provide your credit card number unless the site is protected by Secure Socket Layer (SSL). These sites are identified by https// in their URL.

Encrypting Hardware

The best encryption methods in the world are useless if not routinely implemented. A Computerworld [article](#) just reported a breach at Internet security giant VeriSign. While [VeriSign](#), according to the website, "... enables and protects billions of interactions every day across the world's voice and data networks", this distinction did not prevent an unencrypted laptop containing the personal information of VeriSign Inc.'s current and former employees from being stolen. A security culture is imperative for all organizations. None are exempt

System encryption makes the data of a desktop or laptop computer inaccessible or illegible without a passkey regardless of the application in which the file was created. The passkey should be a complex, yet memorable (to you) combination of letters and numbers. Data encryption should be standard procedure for mobile computing users. [LaptopLock](#) is freeware that protects data by encryption, deleting files and/or hiding them from unauthorized users. Microsoft Windows provides some built in encryption at the file level: [File encryption for Windows XP](#); [Windows Vista and Windows 7](#). Other reliable encryption products encrypt the hard drive of a machine. The free [TrueCrypt](#) can encrypt the disc, as well as peripherals such as external harddrives and thumb drives, and runs on Windows, Linux, Ubuntu and Mac. [PGP](#), the venerable encryption solution, encrypts Windows and Mac OS, as well as peripherals, for a reasonable price.

Lastly, make sure that your backup medium is secure as well. Many portable storage drives will allow you to encrypt the data that you backup. [omega](#), is one manufacturer of smart, portable encrypted storage solutions.

Small storage devices such as thumb drives, discs and the like can hold a tremendous amount of data. But they are also easy to lose. Password-protect these devices, and consider encryption if you frequently place confidential information on them. You can download a freeware encryption software such as TrueCrypt (www.truecrypt.org), or purchase an encryption-enabled thumb drive from Lexar (www.lexar.com). Also, consider a keychain device, lanyard or carrying case.

Laptop Security

Applications known as Remote Laptop Security (RLS) exist specifically to aid in the recovery of stolen laptops. Computrace's [LoJack for Laptops](#) is an example. [GadgetTrak](#) provides anti-theft protection for both PC and Macintosh laptops as well as mobile devices like cell phones and other portable electronics. Most RLS applications require the stolen equipment to be logged onto the Internet in order to be tracked, however regardless of whether or not the laptop is connected to the Internet, [BackStopp](#) will delete pre-selected files as soon as a stolen laptop is turned on.

The best protection is one that prevents a theft in the first place. While more difficult, a laptop computer in a docking station is not a true theft deterrent. More effective are security cables with keyed or combination locks by companies like [Kensington](#). Additionally, the [Targus](#) Security Anchor Base Plate is designed to be attached to a desk or other furniture and further secures and locks down your notebook computer.

The [STOP Security Plate](#) contains owner information encoded in a unique barcode that is adhered to the surface of a laptop computer. The plate deters theft because if removed, it leaves an indelible message on the surface of the computer informing the world that it is stolen merchandise, thus affecting resale value.

A standard laptop case is an invitation to a thief. While traveling with your laptop computer, use a nonstandard carrying case that won't broadcast its presence and then keep an eye on it. There are thieves that specialize in stealing laptops, as discussed in this ABC [article](#). While casual thieves are just looking to make a quick buck, sophisticated criminals are looking for valuable data. If your laptop falls into the wrong hands, make it tough for an unauthorized user to gain access to your laptop's content. Difficult power on passwords that contain a combination of letters, are numbers and special characters are a great first line of defense. Next is data encryption which should be standard procedure for mobile computing users. [LaptopLock](#) is freeware that protects data by encryption, deleting files and/or hiding them from unauthorized users.

Discarding Old Equipment

Discarding or donating an old law office computer is a task that should not be taken lightly. Without properly discarding the information contained on the hard-drive, you may violate your jurisdiction's confidentiality rule. Just deleting everything on the hard drive probably is not enough, as the information can be easily restored and viewed. You should take reasonable additional steps to make sure the information remains confidential.

In most instances, the best thing to do is to reformat the hard drive or use a software utility that "wipes" the hard drive clean. There are numerous products such as Dirk's Boot and Nuke (DBAN), WipeDrive and Sure Delete that are shareware programs (available on [zdnet.com](#)) and commercial products such as Norton CleanSweep. But not all drive erasers are the same. Those that claim they meet Department of Defense standards are probably the best place to start.

If the information on your hard drive is VERY sensitive, then consider removing the hard drive from the computer and keeping it or physically destroying it. Yes, it significantly reduces the value of your donation, but isn't it better to be safe than sorry?

Once you've got your old computer wiped clean of any data from your practice, you may need some help finding a new home for it. There could be many groups in your area, from schools to charities, that would love to have your used computer. If not, you will want to take a look at the National Cristina Foundation (www.cristina.org).

Social Networks and Security

When creating a profile in any social networking site lawyers should be [mindful of how much information they provide](#). By providing enough personal information a thief could easily steal your identity. Likewise, it is not necessary or wise to reveal details about upcoming travel, as it has led to [burglary of a home](#). Likewise [use strong passwords, and do not use the same password](#) for your webmail accounts and social networking accounts.

Be [mindful of scams, hacks, worms, and other things that go bump in the night](#) on social networking sites. News comes out almost daily [regarding exploits and bugs](#) that could lead to identity theft and more. A rule of thumb is always to scrutinize who you allow to become your "friend", block access to unknown or suspicious followers in Twitter, and always be wary of deals that are too good to be true or requests to view videos or links that seem to prey on your curiosity or vanity. Always use antivirus protection, antispyware, and a firewall that protects against incoming and outgoing internet traffic.

Software as a Service

Cloud computing is among the hottest legal technology topics on e-mail discussion lists and in continuing legal education. The appeal of the technology isn't difficult to understand. With applications hosted off-site and the ability to harness large amounts of processing power, cloud computing offers several benefits over using an on-site alternative: manageable monthly fees rather than major initial expenditures; enhanced mobility; simpler, more intuitive interfaces; and easier setup. The virtualization of hardware and computing power enables cloud computing, yet it also is a source of concern: cloud-based services store users' (and their clients') valuable and often sensitive data on vendors' servers, outside of users' direct control.

As set out in Model Rule of Professional Conduct [1.6](#), one of an attorney's foremost ethical obligations is safeguarding her client's confidentiality. So it's understandable that many attorneys are hesitant to entrust their client's data to cloud computing vendors. Unfortunately, there is little official guidance on adopting cloud technologies. Earlier this year, the North Carolina Bar Association proposed an [opinion](#) on cloud-based software, also known as [software as a service](#), but later withdrew it for further consideration. The [ABA Commission on Ethics 20/20](#) is also investigating the topic and is soliciting comment, but formal action may be several months away.

Until attorneys have official guidance from the ABA or their state's disciplinary body, it's important to approach cloud computing with reasonable caution. Attorneys should exercise due diligence in evaluating both the specific services they are considering implementing and the vendors that offer the services.

Before committing to a cloud-based service, there are several important issues lawyers should evaluate:

First and foremost, attorneys should ensure that the product meets their business requirements. While cloud computing can be alluring for many reasons, lawyers shouldn't switch just for the sake of adopting the latest technology. Lawyers should make sure the cloud product offers the features and functionality they require at a price that their firm can afford.

Look for companies that specifically cater to the business market. Consumer-oriented companies tend to be cheaper, better advertised and more common, but they also come with consumer-oriented terms of service and support. Vendors that work exclusively with the legal market will likely have a better understanding of the needs and obligations of lawyers.

What level of encryption does the vendor offer? *When* are files encrypted--before transmission to the vendor's servers or after? Who holds the encryption key needed to decrypt the data? Ideally, data should be encrypted at a high level prior to transmission and only the user should hold the key for decryption.

Ask for a service level agreement. The SLA should spell out, in detail, the vendor's obligations with regard to issues like server uptime, support response time and data security. The SLA should also specify the consequences if the vendor fails to meet its obligations.

Read *all* of the vendor's policies carefully, including the terms of service agreement, and if applicable, the privacy, security and intellectual property policies. In particular, lawyers should look for the vendor's policy on the following key issues:

To whom, and under what circumstances, will the vendor reveal user data? Attorneys should consider both their personal information as a customer and the client data the vendor is housing on the attorney's behalf. If the TOS allows the vendor to share data freely, then the service isn't appropriate for handling client data. Better policies will limit the vendor to producing data only upon subpoena. Ideally, the vendor will also provide the user with notice and opportunity to object prior to release of the data, if notice is permissible by law.

Who *really* holds the data? Realistically, few cloud vendors host their own servers; most rely on dedicated third-party data centers. Lawyers should evaluate the data center's policies, and if possible, the TOS between the cloud vendor and the data center.

How much access do vendor (and data center) employees have to user data? Security compromises are more likely to result from an incompetent or hostile employee on the vendor/data center side than from an outside hacker.

When in doubt, ask for clarification—in writing. If a policy or TOS is unclear, attorneys should not assume that the ambiguities will be construed in their favor. Lawyers should be proactive in upholding their ethical obligations.

The Cost of Free

Recently *Office Watch* reported that 60 Gmail users lost all of their email because of a program glitch. The article then provides some useful instruction on how to backup web-based email to your local harddrive or server. Ironically, if you are not adequately backing up your harddrive or server, it is likely that the online webmail repository will serve as a backup, if the need arises. On January 4th 2007 *The New York Times* published an article by David Pogue entitled "Fewer Excuses for Not Doing a PC Backup". The article describes different online services that offer free and low cost online storage and backup services. While many are lured by the price tag, attorneys must give thought to the potential repercussions of relying on free technology for mission-critical functions.

Free software often provides little to no technical support, or maintenance. Some free software, like Google Desktop Search, can create privacy concerns, depending on its configuration. Free online services in BETA often become fee-based if successful, or lose funding and disappear entirely. Lawyers should be extremely zealous in investigating free downloads and read the EULA (end user license agreement) or Terms of Use to make sure they are not agreeing to download adware or spyware along with the free software, and also check for potential privacy concerns.

As for online backup, while the services mentioned in the *New York Times* article may be useful, online backup providers should be well scrutinized by any law firm considering this backup strategy. The article points out some of the disadvantages, including the time for the initial backup and any restores, security, and corporate longevity. For lawyers add to that the complexities of storing confidential client information with a third party and the repercussions. This is not to say that online backup is inherently too risky for attorneys. It simply means that free and low cost options may not be the right solution.

The next generation of software is going to be on the Internet - call it .Net, ASP, or SaaS (software as a service) - with some distinct advantages. Lawyers need to be ready to take advantage of this model, and be smart about selecting software and services, whether free or fee. When it comes to business applications and backup the price of free could be high indeed.

Resources from Dan Pinnington at practicePRO:

- **Managing Practice Interruptions**

This booklet provides a comprehensive review of the steps you can take to prepare for unexpected minor and major practice interruptions, and how you should respond to them. It reviews what you have to do to protect your people, your practice, and your premises and property.

- **Vulnerabilities assessment chart**

practicePRO has created a spreadsheet chart that you can use to help identify and assess your vulnerabilities. It is available in either Acrobat PDF format or Microsoft Excel format. Included in both of these downloads are instructions on how to use this chart, and a sample chart that includes sample information on a number of common emergencies.

- **Preparing Your Practice for the Unpredictable**

This July 2002 issue of LAWPRO Magazine also focused on disaster prevention and planning. It featured the comments of lawyers at various sized firms with respect to their disaster planning efforts.

All at http://www.practicepro.ca/practice/Practice_Interruptions.asp

Also:

- ***Managing the Security and Privacy of Electronic Data in a Law Office***

Clients, lawyers, and law office staff routinely work with electronic documents and data. Protecting the security and confidentiality of that information is important. Both Rules of Professional Conduct and PIPEDA apply equally to paper-based files and electronic documents such as computer files and e-mail messages. A failure to take appropriate steps to protect the electronic data in your office could result in a release of sensitive information, a malpractice claim, a complaint to the Law Society, or the theft of your personal identity. 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 highlights the risks and provides a comprehensive review of various steps you should take to ensure that the electronic information in your office remains confidential and secure.

-

At: <http://www.practicepro.ca/practice/ElectronicDataSecurity.asp>