

Ten Technology Traps And How to Avoid Them

By:

Mark Bassingthwaighe, Esq.
Risk Management Coordinator
Attorneys Liability Protection Society, Inc.
A Risk Retention Group
mbass@alpsnet.com

Computers are wonderful tools. Their use allows law firms to be far more efficient than they would be without such tools. That said, computers, or more properly, how computers are used can create exposure for a law firm. The following is a list of ten technology traps for the attorney and information on how to avoid them.

1. Laptop Theft

Unfortunately, laptop computers can easily be lost or stolen. Laptop theft is a leading cause of computer security breaches. Far too often, a law firm's computer security measures fail to consider the issues that arise with laptops taken off-site. Here are a few tips worth considering as part of your overall security plan.

While going through security screening at an airport, always keep your laptop in sight. If you go to the restroom or sit down to use a telephone, do not place your laptop on the floor – it is just too easy for someone to pick up the laptop and disappear into a crowd.

Never check your laptop with your luggage. It should always travel with you as a carry-on item.

Tape a business card to the top of the laptop and mark the laptop case to make it readily identifiable and unique. Laptops and cases often look alike, and at some point, you or another passenger might simply pick up the wrong laptop and walk off. This has happened to me.

Never check a laptop into a hotel “baggage hold” room, and do not leave the laptop in your hotel room throughout the day. Place the laptop in the trunk of your car or carry it with you.

Be careful about where you leave your laptop. Sometimes the precautions taken actually result in the loss. For example, instead of leaving a laptop in a cab's trunk with your other luggage, you place it on the floor of the cab's passenger area and then inadvertently leave it once you arrive at your destination. There, the cab's trunk obviously is the better choice. Another way to inadvertently lose a laptop is to hide it in your hotel room, and then forgetting that you hid it when you check out. It's too easy for a laptop to become an out-of-site, out-of-mind kind of thing.

Use password protection on your laptop. If you have a laptop running in a relatively safe but public area, and you need to frequently leave the laptop for varying periods of time, make certain that a screen saver initiates and the system automatically logs out after a period of time – ten to twenty minutes would be a reasonable choice. Don't make it easy for someone to have instant access.

If the laptop contains highly sensitive data, consider using encryption software. Windows 2000 and XP offer file encryption capabilities. There are a number of other products available from independent companies. A few that I am aware of include

Virtual Matrix Encryption by Maganet Corporation, ABC CHAOS (which is free), ImageX from TopLang Software Studio (cleverly hides files by making them appear as pictures), and finally, Encryption Plus Folders from PC Guardian.

Finally, remember to periodically back up the laptop's hard drive for protection in the event that it is lost or stolen. If you do local backups (*i.e.*, to Zip Discs), store those backups separately from your laptop – not in your laptop case, but another place such as your suitcase. Remember, the backup does you no good if it is stolen along with the laptop and its case.

2. Metadata

Metadata in and of itself is not generally a problem as long as electronic documents stay within a law firm. In fact, metadata can be quite useful to individuals who are collaborating on a document. Problems can arise, however, once electronic documents are sent outside a firm.

In case you are unfamiliar with the term metadata, it is extraneous information about an electronic document that remains attached to the document. Unfortunately, metadata is not always visible, and thus it is easy to overlook. As an example, metadata tracked with a document created in Microsoft Office (note: metadata is not unique to Microsoft products) includes your name and initials and the names of your company or organization, your computer, and your network server or hard disk on which you saved the document. In addition to this tracking information, metadata also includes other file properties and summary information, non visible portions of Object Linking and Embedding (OLE) objects, the names of previous document authors, document revisions, document versions, template information, hidden text, comments, macros, hyperlinks and routing information. This kind of information, once outside of a law firm, could be problematic. You might be unintentionally sharing confidential information. Perhaps your true bottom line in a settlement is discovered from a document edit history that has been restored after sharing a document with opposing counsel.

There are products available that will assist in the removal of metadata from documents prior to sending. Understand, however, that a perfect or total solution to the metadata problem does not exist. Metadata is useful and often necessary internally. A solution that completely removes metadata will significantly reduce productivity. The benefit of using metadata removal programs is that they allow you to create a “clean” version of a document that is separate from the original. Caution is in order; however, you must remember to pay attention when selecting which electronic file to send out. Finally, for those of you using Microsoft Office 2003/XP, an add-in is available that will enable you to remove permanently hidden and collaboration data, such as change tracking and comments, from Microsoft Word, Microsoft Excel, and Microsoft PowerPoint files. More information is available at:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=144e54ed-d43e-42ca-bc7b-5446d34e5360&displaylang=en>

Listed below are several companies and their metadata removal product name. This list is intended not to serve as an endorsement of any product. It is simply a starting place in researching metadata removal solutions to meet the needs of your law firm. If you are not already addressing the issue of metadata removal, now is the time to begin.

Esquire Innovations: iScrub
Kraft Kennedy & Lesser: ezClean
Payne Consulting Group: Metadata Assistant
SoftWise: Out-of-Sight

3. Spam Filter Deployment

Imagine that you have a longstanding client who has several open and active matters pending with you at any given time. Also, imagine that your law firm recently installed a Spam filter on the network. You have been pleased to find that in recent days the amount of Spam in your Inbox is significantly less. Now imagine that this longstanding client emails you some relevant information that relates to a time sensitive matter and the Spam filter captures her email. You learn about the email after it is too late to rectify the situation. Is this malpractice? It might be.

Junk email (Spam) is a significant problem and wastes valuable resources including time. One tool in the arsenal used to deal with Spam is a Spam filter. These programs can be quite effective at removing a significant amount of unwanted email. They also often capture legitimate email, particularly in the early stages of deployment. For most law firms, meaning those with fewer than 75 users on the network, consider the following recommendations when deploying a Spam filter.

- Obtain all clients' preferred email addresses for use during the course of representation and provide this information to your technical support personnel. They will enter this information into the filter's "acceptable" list. Going forward, gather this information during client intake.
- Give attorneys and staff access to the Spam filter's quarantine folder so that they can review this folder for email that has been captured accidentally. Any legitimate email that they discover should be added to the "acceptable" list. Again, the sender's email address usually must be given to technical support for this to occur. After a period of several weeks to several months, the task of reviewing the quarantine folder may be reassigned to a staff or technical support person as the amount of legitimate email accidentally captured should be small. Note: depending upon the products in use, the process of moving an email from the quarantine folder to a user's Inbox can automatically add the sender to the

filter's "acceptable" list. Check with your technical support staff for specific instructions for your network.

- Make certain that all who have access to the Spam filter's quarantine folder review the folder on a regular basis. Filters are set up to automatically delete email that has been retained for a predetermined period. Typical automatic deletion periods run from three to fourteen days. Therefore, if the auto deletion period has been set at five days, everyone must review the quarantine folder at least every five days. Review of junk mail is done via a search feature that allows each user to review quarantined email sent to their own email address. Users do not need to review the entire quarantine folder each period.
- Consider placing language in your firm's engagement letters or other introductory materials that request the client contact the firm via phone if an email has not been acknowledged within twenty-four, or forty-eight, hours.
- Require use of the email program's auto responder when staff or attorneys will be out of the office for more than one day and unable to check for email while out. The message sent by the auto responder should contain instructions on whom to contact and how if the matter cannot wait for the staff member or attorney to return.

Spam filters are only part of the solution to the Spam problem. While they can be quite effective at limiting the amount of Spam that appears in your Inbox each morning, filters are really only capable of helping a firm prioritize which email to review first. Filters are not able to determine with 100% accuracy what is legitimate and what is junk. For the time being, this task will continue to necessitate human oversight. Failure to do so could be disastrous.

4. Lack of Professionalism

Email is a place where being casual can be dangerous. Check your spelling and grammar, and make sure your e-mail has a signature block at the end.

Imagine that you are acting as divorce counsel for a client. In all likelihood, given the nature of divorce proceedings, this client will reach the end of your professional relationship feeling emotionally beaten. If, during your representation, this client received emails that were poorly written and rather cryptic, this client will tend toward what all clients do when their case doesn't end quite as expected. The client simply will try to put everything in perspective and often naturally ask himself, "What went wrong?" Unfortunately, the client received your unprofessional emails, and now begins to think, "Why didn't I see this before? My own fifth grader can write better than my attorney can. She's incompetent and my loss is her fault!" Unprofessional behavior can lead to the client questioning your competence.

Professionalism really is about making an implied statement about your competence. In short, professionalism reflects competence. The two necessarily go hand in hand.

5. No Recent Backup

Most law firms understand the need to create periodically a "backup copy" of the firm's computer-based data. There is recognition that hard drives eventually fail, fires and other natural disasters occasionally strike, certain viruses erase data, and computers are sometimes vandalized or stolen. The frequency of creating the backup and the number of backup copies made varies widely. Here are a few thoughts in that regard.

Backup frequency is going to be firm specific. A solo practitioner may not need data backups as frequently as a firm of thirty attorneys may. In a solo practice, the amount of data that is altered day to day is simply less. To determine the backup frequency necessary for your office, consider how difficult it would be to redo the work that has been done since the last backup (e.g. calendaring, time entries, file updates, billing, accounting, etc.). The period of time that you are comfortable allowing to pass sets the rotation schedule. Stated another way, when you are uncomfortable with the time needed to recreate that work, you need to perform a data backup. For small offices, the frequency typically varies between every other day to once a week. For offices of five or more attorneys, a nightly backup is best.

General business standards call for a nightly backup. Typically, the nightly backup is done with a tape-based data storage device, and the nightly backup will use one in a series of five or ten tapes. In a five tape series the tapes are labeled Monday through Friday, and in a ten-tape series the same occurs but with a "week one" or "week two" notation added on the tape's label. At a minimum, keep the current day's backup tape off-site and return it the following workday. NOTE: If you decide to store your backup tapes in an on-site fireproof safe, make certain the safe is rated for electronic media storage. Many fireproof safes will not protect electronic media.

Due to the increase in virus activity and lethality, we strongly recommend keeping a second series of backup tapes. This second series of tapes should be a minimum set of three tapes and often goes to six. Use these tapes to create monthly backups and label accordingly. This entire series is stored off-site. The rationale for this second series is that a virus could infect the firm's computer systems and copy itself to the daily backups, potentially rendering the daily backups useless. If there is no secondary monthly backup tape, a virus-infected daily backup tape creates a very serious problem for the firm because it will likely be useless. After a virus attack, if you have a secondary monthly backup tape series, one of these secondary tapes should be virus-free, allowing partial recovery of the computer system. A partial recovery with the loss of perhaps two months of data (the last virus-free tape) is far better than no ability to recover data and programs. Some firms permanently archive a monthly or quarterly backup tape, and that system can be just as effective as the monthly duplicate system.

Occasionally a firm refuses to do the secondary backup series because of tape costs. We believe that this is an unwise economic decision. Consider the cost to rebuild your entire database from scratch, and then compare the cost of backup tapes. Some of our insured firms have actually faced this situation and were forced to rebuild their entire damaged computer systems. Those firms now use a different backup procedure. In short, a few dollars per month for a tape is cheap insurance.

An often overlooked but very important step is monthly testing of your backup tapes. It is imperative that you periodically try to restore some files to a test area on your network, or to a test server, and then open and use the stored backup files to ensure that the information is there, is accessible, and is usable. Once a year, and soon after implementing a new backup system, you should use the backup tape to do a full system restoration on a test server or in a designated test area, to ensure that your backup contains everything needed to run and use your computer system. There are horror stories of firms that diligently did nightly backups, but when disaster struck, they found that their backup copy was blank or was not backing up the data that they needed the most.

One final comment -- all backups should be full backups, and not merely a fast update of altered files only. Although partial backups initially might appear to save time, they can create long-term problems when trying to rebuild the system after a disaster. Partial backup tape volumes can have thirty or more updates on them, and trying to rebuild your system's data from such a tape, often will prevent you from fully recovering your system's data and operability.

6. No Legacy Systems

My first computer came with a built-in 5 ¼ inch floppy drive and the new 3 ½ inch disk drive. I was tremendously excited. Of course, this was a DOS based system and I spent more than a few hours learning how to do some programming in DOS. During that time, I copied a number of files to floppies, such as a resume, and had some great programs that came on floppy disks. Several of these programs were wonderful educational programs that I enjoyed playing with my firstborn.

Over the years technology continued to improve and I went through several computer system upgrades as my family and perceived technological needs grew. When my youngest was born, I dug out some of the old programs only to realize that I had no longer had a 5 ¼ inch floppy drive with which to access the programs. With a little work, I did manage to locate one and successfully copied the program files onto more current media only to find that the programs, not to mention my files including my resume, were not compatible with the current operating environment of my new system. It would seem that not only did hardware improve over the years significantly but software improvements had occurred as well.

This wasn't a crisis. I could live without the programs or the files that I had made. Yes, it did take a little time to re-gather information since I now had to redo my resume but I could live with that. This scenario, however, would play out quite differently if the old files and programs were business related. Consider all the scanning that is being done now. It may be ten years, fifteen years or even more but at some point, you may have a pressing need to access the data being scanned now. The question then becomes, will it still be accessible at that point? Will CDROM discs still be in wide use? What about the storage software programs, will they still be supported? Will those programs even run in the virtual environment of that time? I was one who thought that 8-Tracks and Beta Video would always be around. Who knows for sure? In reality, no one.

This leads me to the following suggestion. As you develop paperless systems discuss the long term access issues with your IT staff or consultant including the option of maintaining a legacy system and legacy software. As you upgrade and/or replace systems, consider maintaining a standalone PC as the system exists today. In other words, keep a current PC configured with the hardware and software in use today in a file storage location to be available for accessing current data files down the road. Original software programs, including the original recovery and restore disks should be kept in a safe place. Then, if years down the road the electronic data storage files being created today are no longer accessible on the then current system, you have a legacy system with which to access these files.

Another idea might be to store files in widely used formats such as tif or PDF because they will likely have a longer life span. Printer drivers that save files in a tif format are available from Informatik (www.tiffdriver.com) and they are inexpensive. An Adobe Acrobat program (files can be written in PDF format) is also available for under \$200.

One will never know the direction that technology developments will take, in part because it seems so difficult to predict what technologies will eventually take hold in the marketplace. However, this is one of those ideas that will cost little money and thus might be very worthwhile considering. The money has already been spent on existing software and hardware. The idea is simply to keep a small part of it when systems are upgraded and replaced. Yes, this idea runs counter to the practice of "out with the old, in with the new" which seems so prevalent in technology; but in this instance it is probably a good idea. If nothing else, this is food for thought each time you upgrade your office system.

7. Misdirected Email

Email occasionally is sent to the wrong recipient. As a result, attorneys routinely place an email disclaimer at the beginning or the end of an email text. The disclaimer language is similar to the "misdirected fax" language so often placed on fax cover sheets. The ten-dollar question is, "does the disclaimer actually accomplish anything when a confidential email unintentionally lands in the hands of opposing counsel?" In reality, the answer is "no." Granted, you can find one or two ethics opinions that will say that the receiving

attorney should not read the email beyond what was necessary to realize that an error had occurred, should notify you of the error, and should delete or return the email as instructed. Of course, the erroneous recipient should not use anything learned from the misdirected email, and he should forget everything he read on that email.

Although many attorneys will behave admirably and abide by such ethics opinions, a harsh reality is that others will not. In the end, attorneys in most jurisdictions have to live with the effects of their mistake. Perhaps informing the malpractice carrier would be prudent, but beyond that, the attorney must realize that his mistake cannot be undone.

I recognize that among the emails sent into and out of law offices, the majority of them do not contain highly confidential information. This means that most misdirection errors will not likely cause significant harm to the client. However, when you need to send your client some highly confidential information via email, and you aren't using email encryption, there is an alternative. Consider using an electronic "envelope within an envelope" approach to email transmission, and keep a record of the emails sent using this approach.

The "envelope within an envelope" approach works as follows. The confidential information is sent as an attachment, and the text of the email contains only the email disclaimer language and information that identifies the intended recipient and specifies what the attached document is. If the email is mistakenly sent to opposing counsel, she is on notice that the attached document contains information not intended for her eyes. If she opens the document anyway, you may have a valid argument that opposing counsel should be dismissed from the matter, or at least should be prevented from using the information that she obtained unethically. Of course, we cannot guarantee that the argument will succeed, but surely it is better than no option at all.

8. Delete is not Delete

Far too many computer users still mistakenly believe that deleting a file permanently removes the file from the computer, making it unrecoverable. Even more troubling is that users who do understand that "delete" isn't really a full delete still do not take appropriate steps to prevent discovery of potentially damaging information. You may recall that in the Microsoft trial, Bill Gates had "deleted" email come back to haunt him. Don't learn the hard way that "deleted" information can be recovered from hard drives.

Files that are deleted do remain on the hard drive. Deleting a file simply erases the file name and a "pointer" that directs access to the file's location. The "deleted" information may remain on the hard drive indefinitely if the computer does not need the space that "deleted" files occupy. Even reformatting a hard drive will not prevent recovery. In order to fully remove the "deleted" information from your computer, you must "electronically shred" the information. Overwriting the data with gibberish will accomplish this. The U.S. Department of Defense has established an electronic

shredding standard known as DOD 5220.22-M. This standard requires that a file be overwritten seven times, using a different set of random data for each pass.

In order to make certain that deleted files, unwanted email or Internet use histories are inaccessible even to a forensic computer expert, you must overwrite the data. There are a number of programs available, and you can download some of them for testing before you buy them. A few products that meet the DOD standard and are worth a look include Active@KillDisk (www.killdisk.com), Zdelete (www.zdelete.com), Shredder 95/98/NT (www.gale-force.com), DataEraser (www.ontrack.com), Ultra Destroy-IT! 2002 (www.blcorp.com) and Bestwipe (www.jetco.com). If you wish to wipe the entire drive clean for any reason, look at a product like WipeDrive (accessdata.com). Remember – you should research and review any software product *before* buying, to ensure that it addresses the specific needs of your practice.

9. Failing to Take Care of What Antivirus Programs Miss

I'm sure most of you are familiar with antivirus programs that help prevent a virus or worm program from contaminating your computer. However, viruses and worms are not the only forms of threatening software. There are other types of programs that are potential security risks. Many people refer to these other programs as “malware.”

Most computer users are unaware of malware programs because they do not necessarily damage a computer system, and they quietly download from the Internet in the background and run in the background, usually without the user's knowledge. Malware programs come in different forms, and can include such malicious functions as password crackers, spyware that monitors your internet activity and relays that information back to a third party, virus creation tools, and “adware” that creates those annoying advertisement “pop-ups” that keep appearing on your monitor's screen. Other types of malware programs enable a remote computer to monitor your machine or scan your computer network. If you ignore malware programs and let them remain on your computer, undoubtedly they will increase your security risks.

PestPatrol, Inc (<http://www.pestpatrol.com/>) offers a software solution to the malware problem. Not surprisingly, they call the software “PestPatrol.” It's a highly customizable program that identifies and labels as “pests” the programs and files that pose potential threats, and lets the user determine which files or programs to remove. The program provides users with information on every threat that it has located, and provides several options for dealing with those threats. The options include ignoring the files that you wish to keep, deleting the “pest” entirely, or quarantining the “pest” until you further research whether you want to delete that “pest.” Also, the program provides a link to the PestPatrol internet site for additional information about the pests that PestPatrol identifies on your machine. Two similar programs worth considering are Spybot and Ad-Aware. You can find information regarding Spybot at <http://www.safer-networking.org/en/download/> and Ad-Aware at <http://www.lavasoftusa.com/software/adaware>.

You should not use a malware detection and removal program like Spybot or PestPatrol in place of general security programs such as firewalls or antivirus programs. However, if you use programs like Spybot or PestPatrol in conjunction with general security programs, you can further tighten the security of your computer systems.

10. Delete is not Delete – Revisited

We learned above that deleted files don't go anywhere once deleted. Unless deleted files are appropriately overwritten, they remain available for possible discovery. This could be disastrous for a law firm.

At the end of the day all network users must abide by a simple rule while on the firm's network or using any computer that might touch the firm's network such as a Blackberry, PDA, laptop, or home computer that is used for business even on a limited basis. Potentially, the information on any of this hardware is discoverable in a malpractice claim just as one example. The rule is this. If you are not comfortable having a personal or work related email read by a jury, an electronic note to a file read by the client, or your personal browsing history known publicly don't write the email or note and don't visit the Internet site. Clients have obtained copies of email that should not have been written, juries have been presented with incriminating email, and careers have been ruined once personal Internet browsing habits became known publicly.

For all practical purposes, users are recording everything that they do on a computer and erasing the record once created can be extremely difficult. Worse yet, electronic erases leave their own record of events. Responsible use of technology is the safe play.

Now, two thoughts for good measure....

11. Mirrored Hard Drives – The Overlooked Redundancy

Most law firms are backing up their computer data and taking copies of the backup media off site. Occasionally I will visit a firm that relies solely on a "mirrored" hard drive as the system backup, and this isn't wise. A "mirrored" hard drive is a complete copy of your primary hard drive. For reasons I will describe below, it is not the most reliable system backup. Few firms have both a mirrored hard drive and a remotely stored medium holding the backup data. In this tech tip, I want you to consider doing both.

Back up media are necessary for a catastrophic event (such as a fire) in which your computer network is destroyed. If you have a reliable off-site backup copy of your system data, you can buy new computers and simply upload the system data from the backup media.

On the other hand, a mirrored hard drive usually is an internal device, and you cannot easily take it off site. Thus, a fire will destroy the mirror drive along with the rest of the system. This is why internal mirrored hard drives are not particularly effective as the sole device for system backup. Still, you should consider using both a mirrored hard drive and off-site backup media. Here's why.

Hard drives fail. Buying a new hard drive, installing it, and uploading the data from the backup media will take some time. Don't wait for a hard drive failure. Take some time right now to consider the following questions.

- If your network drive failed, how soon would you need access to your computer data?
- Can you obtain a replacement hard drive quickly, easily and locally?
- Is your IT consultant immediately available for emergency installation of a new hard drive and the associated network restoration?

If these questions make you realize that you truly cannot afford to have your network unavailable for much more than a few hours, then you should consider using a mirrored hard drive in your network. There are a variety of ways to run a mirrored hard drive, and your needs and network configuration will dictate which option is best.

Consult your IT support person and seek his or her recommendation on a mirrored hard drive for your network. A mirrored hard drive can enable a quick and easy hard drive swap after a hard drive failure. You simply substitute the mirror drive for the failed drive, and you are up and running with minimal down time. If you already have the mirror drive installed, switching over to the mirror drive is simple. You can train a staff person to do it, for those times when your IT consultant is unavailable.

Once the mirrored drive is running, you will have the time to get a replacement drive. Your replacement drive will become the new mirror drive. The cost of this redundancy is reasonable for most small businesses, particularly when you consider the cost of not having your network available for an extended period of time. Don't wait for a hard drive to fail. Give this measure some thought, and actively prepare for such a failure.

12. There Is Such a Thing as an Electronic Watermark

Imagine that a client comes to your firm to have a contract drawn up. Once the draft document is prepared, it is forwarded to the client electronically for review. At this point, the client drops out of contact. He made a decision to run with the draft version on his own in order to save the time and expense of keeping an attorney involved. Of course when something goes wrong this client will seek to hold the attorney accountable for the error.

Problems like this can be avoided through the use of electronic watermarks. It is possible to insert watermarks, which are pale images or text, behind the text of word processing documents, behind the text in PDF files, and even over photos. Watermarks document the conveyance of information to the recipient of the electronic information and the watermark stays on the document when printed. Further, if set up correctly, the recipient should not be able to edit the file in an attempt to remove watermark.

The process of adding watermarks to word processing documents varies by program and, unfortunately, even by version of program and can be somewhat time consuming. Therefore, consider creating several preformatted document templates that can be selected for use whenever needed. You might create a template with the word “Draft” as the watermark. Other templates could be formatted to say “Priority,” “Do Not Copy,” or “Confidential.” Instructions for how to create these templates can be found on the Internet or seek guidance from your IT staff or IT consultant, as this isn’t a one or two click procedure.

While Adobe Acrobat is designed to allow for the use of watermarks, a number of firms do not use Adobe Acrobat. Thus, to add a watermark to a PDF file or a photo, you will need to obtain software designed to perform these functions. There are a number of programs available for purchase and as shareware that don’t require that you have Adobe Acrobat. One program that I like is PDF Toolbox 6.0 available at www.clicktoconvert.com. Again, there are a number of others worth investigating.

The goal with this tip is to make you aware that a programming solution exists to an age-old paper document problem. While we can’t stamp electronic files, electronic watermarks can accomplish the same purpose. The investment of a little time and energy now may save you from a real headache down the road.