

# 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](mailto:mbass@alpsnet.com)

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 XP and Vista offer file encryption capabilities and there are numerous other products available from independent companies.

There is still one line of defense that could be deployed to try to mitigate the damage after the laptop is gone. Stealth software programs are available that enable a tracking center to locate your laptop (once reported as missing) whenever the missing laptop is connected to the Internet. In short, these companies work with the authorities and Internet service providers to track and recover your laptop. A few programs also allow you to retake control of your data even though the laptop is no longer in your possession. You are thus able to remotely recover, delete or encrypt sensitive files while rendering the missing computer useless by locking the keyboard and mouse.

If a lost laptop would be a nightmare for you, consider using this line of defense. The costs are reasonable. Several companies worth considering are listed below:

zTrace Technologies at [www.ztrace.com](http://www.ztrace.com)  
Absolute Software at [www.absolute.com](http://www.absolute.com)  
Stealth Signal at [www.stealthsignal.com](http://www.stealthsignal.com)

Given the number of laptops reported stolen each year, I would consider this money well spent if your laptop contains any sensitive information at all. A call to inform your client that your laptop was stolen and the client files were not encrypted is a call I would not want to make. This approach might make that call a little easier should the worst happen.

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 Flash drives or external hard drives), 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

concern if the computer network is appropriately secured. While a program could be introduced behind the firewall, the security programs running on the network will in most instances catch the intentional or unintentional installation of a virus or other malware.

The real concern for me is the unauthorized and covert removal of files. Think how easy it would be for a disgruntled employee to download files to an iPod Nano and slip it into a pocket and walk out the door. What if someone offered to pay an employee for copies of electronic files? How would you ever know the data had been stolen? When you consider that the new iPod, just as one example, has a 160-gigabyte drive, the amount of data that could be copied and taken is quite large.

One approach of addressing the concern would be to consider banning or restricting the use of portable storage devices through a written policy. Established guidelines enable you to define what is appropriate and not appropriate in terms of what types of devices are acceptable and when or how they may be used. This would also allow you to establish a security policy that might mandate using only devices that are password protected and/or encrypted, require that only devices provided by the firm may be used in the office and that the devices must be signed in and out.

While it is possible to disable USB ports on some or all PCs within a firm or to restrict the use of portable storage devices to a read-only format, such steps are in most instances possible only through the use of third-party software. Fortunately, the number of products coming to market are increasing and getting better in terms of options and capabilities. My best advice, if you wish to go beyond just establishing a policy, is that you discuss the issues with your IT consultant and learn what your options are.

#### **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.

Before going any further, however, I want to be clear in stating that if a tape based backup system is in place at your firm and is working for you then stay with it. Backup digital tapes properly created, rotated and stored can result in a reliable backup process. This tip is directed at those of us who fail to consistently follow through with tapes for any number of reasons. The low headache factor, highly reliable alternative is online backup. An online backup service provider conveniently and automatically handles the creation of backups, backup removal off site via the Internet, secure data storage and reliable data recovery if ever necessary. Online backup services are not foolproof and there are significant cost and service differences out there so a little investigation is in order to find the solution that best fits your law firm needs. At the end of the day however, I feel that established online backup service providers are able to provide a level of expertise and security that most of us are unable to bring to the table.

If interested you might begin by checking out these providers (and there are many others):

IBackup at [www.ibackup.com](http://www.ibackup.com)

LiveVault at [www.livevault.com](http://www.livevault.com)

Evault at [www.evault.com](http://www.evault.com) and

Data Protection Services at [www.dataprotection.com](http://www.dataprotection.com)

## 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

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 which requires that a file be overwritten multiple 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. A few products that meet the DOD standard and are worth a look include Active@KillDisk ([www.killdisk.com](http://www.killdisk.com)), Zdelete ([www.zdelete.com](http://www.zdelete.com)), Ss Data Eraser ([www.ss-tools.com/data-eraser](http://www.ss-tools.com/data-eraser)), and DriveZapper Pro! ([www.wincleaner.com](http://www.wincleaner.com)).

good idea, particularly if that someone happens to be an attorney talking about a client's matter. Remember Rule 1.6 of our Rules of Professional Conduct which speaks to the duty to maintain client confidences? Convenience doesn't negate any of our professional responsibilities. So let me say this again, and consider the advice in the context of how you use any tech gadget, be it a digital phone or a wireless laptop in public hotspot. Just because you can do something, doesn't always mean that it's a good idea. Be responsible in how you use any tech gadget. The failure to do so has already led to very bad outcomes.

## **10. Careless Use of Individual Attorney E-mail Hyperlinks on Firm Websites**

Websites have gained wide acceptance within the legal profession and for good reason. I have long since stopped picking up the Yellow Pages for information about a local business preferring instead to turn to the Internet and I suspect that I am not alone in doing this. While the business and marketing justifications for creating a web presence are fine, a failure to address the potential risks associated with a web presence can lead to trouble. One common misstep is in the posting of individual attorney e-mail hyperlinks on a firm's website without effective disclaimers. Caution is in order.

Here is one concern. A law firm's website can easily be perceived as manifesting the intent to offer to form an attorney-client relationship via e-mail. When someone acting on this offer sends an e-mail to the firm, is this person now properly viewed as a prospective client triggering confidentiality and conflict concerns? Ethical opinions are saying yes to this question. While there are a number of ways to address this concern, a common approach is to rely on a disclaimer of some sort and it is the use of this tool on which I'd like to focus.

A widely used tactic is the placement of a disclaimer on a website's homepage hidden behind a disclaimer hyperlink. This is a passive approach to the problem. I don't know about you, but I typically don't take the time to look for and read buried disclaimers when I'm on the Internet. My point is that neither does anyone else. Making matters worse, I have viewed website "terms of use" disclaimers that are so long, convoluted, one-sided, and full of mind numbing legalese that the disclaimer has in all likelihood become entirely ineffective. In short, I would suggest that there is no enforceable agreement with these things. Yes, reasonable minds may see this issue differently. I just don't want you to be a test case. If you take the passive approach, treat unsolicited e-mail as coming from a prospective client. This means that even if no attorney/client relationship is created post receipt, the information shared is confidential regardless of what your disclaimer states. Also, be aware that you and the firm may have a serious conflict problem if you already represent the opposing party or are ever contacted by the other side.

The alternative is in taking an active approach. Require an affirmative assent to the disclaimer before allowing for the transmission of an e-mail to you. In other words, force the prospective client to "click" on an acceptance of the terms of the disclaimer. Now at least it is possible to avoid the unintended disqualification of the firm based upon the

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. A Password Conundrum**

At times, I feel that passwords are to the average computer user what bad tasting medicine is to a sick child. If only we didn't have to take it! Most of us, however, have come to recognize the value of having a strong password policy (e.g. use of alphanumeric passwords) in the workplace setting. After all, how many times have we all been told, "Never write your passwords on a sticky note and tape it to your monitor?" Unfortunately, holding one's nose to get the medicine down, if you will, can lead to an unexpected problem when it comes to following through with strong password policies.