

Barbarians at the Gate: Top Tips for Keeping Your System Secure

By:

Ross L. Kodner

©2004 Ross L. Kodner, All Rights Reserved

May 12, 2004

Electronic security and disaster prevention are facts of legal life today. With new computer viruses and daily security breaches, protecting client confidences and firm information is challenging. Complicating this is the HIPAA privacy legislation. Security and disaster planning are as critical in small firms as in mega-practices. This article explores seven quick tips for practicing safe computing:

1. Know your responsibilities: ethical rules are essential reading. Review for applicability to issues related to security and protection of client information from loss or intrusion. Pay attention in ethics credit CLE programs. Leverage the knowledge of your state bar ethics advisor. Talk to your malpractice insurance carrier and get their opinion, in advance.
2. Understand HIPAA: the healthcare privacy requirements in this legislation impact lawyers in many areas - not just those that are injury or healthcare-related. Lawyers and clients are subject to significant penalties for failing to protect the privacy of healthcare information.
3. Backup - not optional: the need to backup should be a given after years of pleading and begging. Many small firms still have inadequate systems for backing up firm and client information. The ability to access the data (i.e. backing up your programs to enable quick restoration to normal operation) is as important as protecting data. Occasionally copying your documents to a writable CD isn't an adequate backup system; it's a malpractice action waiting to happen. Whether via tape or external/removable hard drives, employ purpose-built backup software, off-site backup storage, alternating media, and regular test restores.
4. Security - it's not someone else's responsibility: so you have a shiny new cable modem in your office. The cable guy told you they've got that whole "security thing" taken care of - great news! WRONG! Security is YOUR responsibility - it's your business, your practice, your obligation to protect the integrity of your client information. Use a hardware or software firewall to protect your internet connection from hacking. There are even "free" software firewalls available from vendors such as ZoneLabs (ZoneAlarm

Standard) and Sygate (Sygate Personal Firewall). More preferable hardware firewalls can be had for as little as \$100 (i.e. using a cable/DSL router device that also has built-in Network Address Translation (NAT) and "stateful packet inspection") although this is considered "barely adequate" (look for firewalls that also incorporate a technology called "stateful inspection"). So cost shouldn't be the reason that you throw security caution to the wind. Get firewalled, period.

5. Security is an attitude: You can buy the most secure firewall products in the world but if you write passwords on Post-It notes stuck to your monitors, nothing will protect you. Think of the people (i.e. cleaning crew) who visit your office after hours. Security is, foremost, procedures created and enforced by top firm management. All the technology invented won't protect you from lax policies.
6. Viruses: e-criminals distribute new viruses every day. Averting professional disaster means taking precaution against virus infection - or spreading them to others. Could you be liable if you didn't update your anti-virus software, thereby becoming infected and in turn, infecting a client whose business is shut down for days? You bet you could be. Four tips: a) use capable anti-virus software, b) update it automatically, DAILY, or even multiple times per day, c) educate your people about not inadvertently spreading viruses and the liability your firm could incur from infecting other companies, courts, clients, etc., and d) never trust just one person to keep your anti-virus software update subscription current – it's not the software that let's most firms down, it's the liveware (the people!)
7. Plug the holes: you need to keep your operating systems, your applications and your Internet software updated with the latest patches. Microsoft products are regular targets of hackers. You can counter the troublemakers with Microsoft's free Security Bulletin Alerts. This e-mail based service warns of the latest security and privacy issues affecting their software and links you to the needed patches.

For all the law practices now using Microsoft Word as their document generation system, there's a horrifying threat that needs to be addressed: it's called "Metadata." From the time a Word document (or an Excel spreadsheet or a PowerPoint file) is created, through all the edits, revisions and modifications that occur during the life of the document, a frightening amount of information is permanently stored, invisibly, "under the hood" so to speak, in the file. Anyone who knows how to view such a file (as easy as selecting the "Recover Text from Any File" option in Word's "File | Open" dialogue box, whereupon retrieval of the file, all the contained metadata is tacked onto the end of the document) can exploit it to their advantage. For example, assume you've had several revisions of a document with passages of text being removed, copied from other documents, comments

inserted and deleted, etc. Perhaps some of the language, or even the entire document was [leveraged] from work done for another client. If that document leaves your firm as an e-mail attachment, what are the consequences of someone outside your firm being able to view all the information you thought was no longer there? Have you breached client confidentiality (of both the client in question as well as the earlier client whose work you recycled and whose information is still hidden in the document)? Could this be an ethical violation? How about malpractice?

The only practical ways to address this issue are to turn Word documents into PDF files (using Adobe Acrobat writer or an equivalent compatible product such as FinePrint Software's pdfFactory Pro), which strips virtually all the metadata out of the document. Or alternatively, use a Word add-in that removes Metadata from documents such as Metadata Assistant from Payne Consulting (or MetaWALL from Workshare Technologies or iScrub from Esquire, Ltd.). The point is, in the "protecting your clients from disaster" category, taking one of these approaches must be considered mandatory.

The bottom-line: we practice law in a complex electronic environment. Protecting our confidential information can't be an afterthought - it must be as rigid a daily procedure as entering time. It is essential that your law strive to "practice safe computing."