Is Your Firm's Computer Security Policy Compromising You?

Copyright 2016 by Richard Schenkar

The process of thinking through your firm's computer security policy allows you to take control of your network and integrate it with the management of your firm. Ultimately, lawyers are responsible for the network, the firm, and their licenses to practice law. The thought process makes your system and network more reliable. Reliable systems generate client satisfaction and cash flow.

Consider the following issues when creating your computer security policy:

Acceptable uses: In this category of considerations comes the access to pornographic or other sites that might be considered to create an oppressive workplace (that could lead to firm liability). A more complex issue is how to handle access to sites that would ordinarily be forbidden or disallowed, but the nature of your practice issues create legitimate reasons to access material. For example, if your practice involves research on gynecology, you may discover that a number of web sites offering helpful information are blocked by software that some administrators load on systems to enforce an acceptable-use policy. Make sure that any rules you create do not limit access to material that would be of value to some attorneys. Like many issues, this one involves trust. If one understands the reasons for the rules and one is willing to avoid the problems the rule is trying to combat, then there is no problem and one does not need a rule.

Passwords: Passwords are literally the key to your computer system and they can keep out most of the challenges to system security. Make them long, make them complex, make them memorable, and change them often. Longer passwords are harder to discover or crack. The person seeking to get your password uses software that can try many combinations of letters and numbers; the more characters there are, the longer it takes to figure out your password. Complexity keeps your password secure. Mix letters, numbers, upper and lower case, and other allowable characters in a hard- to-guess matrix. Make them memorable by taking advantage of

songs, favorite thoughts or phrases that keep resonating in your mind called earworms to frame pass-phrases that you can remember, then add enhancements like changed characters or other modifications to make them hard to guess.

Electronic mail: Your policy considerations here include handling attachments, encryption of e-mail, storage, archiving, indexing, and retrieval. As many corporate executives have discovered recently, e-mail on their own systems can be read back to them at trial to their embarrassment or their liability. Remember that e-mail is not really confidential. Although the American Bar association has said that unencrypted e-mail is acceptable to use in the practice of law (in its Formal Opinion 99-413 (March 10, 1999)), your standard of confidentiality may suggest a different standard. Consider what software you will use to encrypt, the clients with which you will communicate offering this encryption, and how you will communicate with the client about the encryption process.

Web site use: here, consider what you want to post and when, any updates or continuing RSS (really simple syndication) feeds that offer continuous new content. Ask yourself who you want to attract to your site and how that person will feel most comfortable. And write that into your policy.

PDA use: Personal digital assistants are becoming more prevalent in law firms. The challenge is management and reasonable standardization. If possible, get your law firm personnel to agree on hardware and software so that files generated are compatible across the firm's network. Since it is hard to get personnel to agree on everything, at least make sure the files generated by all the hardware your firm members use can be managed or converted to formats that other personnel can use.

System maintenance: Three major issues to cover in your policy include antivirus scans, spyware and malware scans, and file-deletion policies. Antivirus scans are necessary because it is easy to acquire viruses by any Internet access and the viruses can lay dormant on your system for any period. Plan to run an antivirus scan once per weekâ€”more often when threats are common. Seek out an antivirus program that provides virus

signature updates and update the virus signature files before running the software on your system to make sure you care catching the more recent virus threats.

Spyware and malware are also special threats: Spyware is software that can capture and send confidential data to other computers. Malware is software that destroys software or disables hardware. Run scans for both of these threats weekly and place that rule in your policy.

File Deletion Policy: Most people do not realize that to delete a file on a computer disk just changes that status of one flag in the disk index (called the file allocation table). There is a whole forensic file-undeletion industry that has sprouted to find that flag on computer disks, change the status of that flag, and make deleted files instantly visible to someone's occasional discomfort. There are utilities that will completely erase files to U.S. Department of Defense high-security specifications so that they cannot be retrieved and use of these utilities should be considered in your law firm's security policy.

Remote access: Are you going to set up a local area network or a virtual private network? Are you going to let law firm personnel access files from remote locations like coffee shops, courtrooms, or home? Be sure to secure the network access point and, especially, secure the tools law firm personnel use to access your law firm network. Attackers tend to go after the least secure element like the laptop computer, PDA, or cellular telephone used to access your network and use that as a conduit to get into the heart of your network. Make sure your remote use tools are secure and protected.

Wireless access and use: Even if you do not have a wireless network, have a policy about its use in remote locations like cafes, courtrooms, trade shows, and other public areas where wireless access points are becoming common.

Storage: What tools will you use for file storage? Do you have some organization for files so that they may be retrieved easily? Consider the nature of your practice, the kinds of data you will be storing and the way you think about your practice and set up a system of categories that will work for you. Document your policy for storage and deletion.

System backups: These will save you hours of typing or frustration. Have a backup policy. Keep backups on removable media. Most compact-disk drives will write to a proprietary format, but, when ejecting the disk, will allow you to have the material rewritten to be read by most CD-ROM drives. This way, if your CD drive malfunctions, you will be able to read the material on other drives.

Incident response: Plan what will happen when you are invaded or when you have a security incident. Have a list of people you will call, with telephone numbers and other access methods.

Also consider when and how you will allow exceptions to the policy you are writing. Remember, this is an evolving document, so keep revising it and do a comprehensive review every three months. For language you can use in your security-policy document, refer to http://www.sans.org/rr/whitepapers/policyissues.