Technology — A New Ethical Risk

By Andrew Beckerman-Rodau

What happens when your computer system crashes and you lose client data? Or client data is inadvertently accessible to third parties? From a business perspective this can make for a very unpleasant conversation with clients. Additionally, ethical rules may be violated. Typically, ethical obligations require an attorney to take reasonable steps to safeguard client information and to prevent inadvertent or unauthorized disclosure of such information. An attorney is also required to use reasonable efforts to insure that non-lawyer employees of the attorney comply with these ethical obligations.

Frequent media coverage of the risks of reliance on computer technology means the general public has at least a general awareness that some level of protection must be utilized to protect computer systems. Hence, failure of an attorney to become educated about such risks or to engage appropriate personnel to minimize such risks is likely to be considered unreasonable conduct either today or in the very near future.

Professor Beckerman-Rodau is professor of law and co-director of the Intellectual Property Law Concentration at Suffolk University Law School. He is also an engineer and registered patent attorney. Professor Beckerman-Rodau is admitted to practice in Ohio and Massachusetts.

The pervasive use of modern technology has resulted in law firms and corporate law departments increasingly creating and maintaining files, litigation materials, confidential client information and other data in digital form. This form of data is easy to update, transfer and search so it can save time and increase efficiency while minimizing errors. Nevertheless, certain risks accompany use of digital data. An attorney must be cognizant of these risks to avoid the potential for violating ethical obligations.

A computer system can be viewed at its most basic level as an electronic storage cabinet. Additionally, if the computer is networked — which is common in most firms today — it is analogous to the door to the firm's file room. An attorney would not leave individual files or access to a firm's files open to the public. However, an unattended computer is the equivalent of leaving access to a firm's data open. During the workday, employees, vendors installing software and technical personnel may have access to computers. Additionally, after business hours, both maintenance staff and cleaning contractors routinely have access to office space, which gives them access to any unattended computer.

At a minimum, individual computers should require passwords for access. The ability to set passwords is built into most software. But merely requiring passwords is inadequate. Many individuals use names, addresses, phone numbers or similar data to make it easier to remember the password. Unfortunately, this often makes it easy for an unauthorized person to guess a password. It is also common to see passwords written on Post-It notes or written on the inside of desk drawers, which is akin to hiding a key under the flowerpot. One simple method of creating better passwords is for users to remember a long sentence where the first letter of each word makes up the password. A long personalized sentence will be easy to remember but it will result in a random password that is hard to guess.

In addition to securing computers, portable media such as floppy disks, Zip disks, CDs and backup tapes should be secured. At a minimum, such media should be kept in a locked desk drawer or file cabinet.

The increased use of wireless connections is a great cost-saver because it allows networking of computers without the expense of running wires. Additionally, it allows an attorney to access the Internet and the office network while traveling. This is becoming increasingly popular now that many airports and hotels provide wireless access. However, such easy access may also allow unauthorized interception of data and access to a network connected to a wireless system. Although a wireless network cannot be completely locked down merely turning on the security features incorporated in wireless equipment, it can significantly reduce the risk of unauthorized access. Typically, wireless equipment is shipped with all security settings turned off. These default settings can only be changed by the user turning on the security features.

Maintaining the integrity of computer data is critical. This avoids the loss of data due to a computer crash or other malfunction. The primary precaution is backing up all data on a regular basis. Backup procedures can be elaborate or basic. Largely, the decision is based on both the importance of the data and the potential economic consequences if it is lost. Data storage companies exist that can provide off-site storage in highly secure and remote facilities. Data can be sent to such facilities over encrypted Internet connections on a daily basis. Alternatively, current tech-

nology makes it both easy and inexpensive to backup data locally. Large capacity but inexpensive external hard drives can be plugged into the USB port, common on all computers today. Simple backup software can be installed to automatically backup all data onto this external hard drive. Such hard drives can also be connected to a computer network so it will backup the data on all networked computers. Typically, a backup system must be setup to operate automatically in background rather than relying on computer users to manually activate it.

Storage of files is useless if they can't be accessed in the future. Technology advances rapidly but often older data formats are not supported by newer software. This is a common problem referred to as lack of legacy support. Hence, in addition to backing up data, old versions of software must be maintained to insure access to backed up data.

News media carry frequent accounts of technological assaults on computer systems by viruses and malicious software called spyware or adware. Some simple precautions can substantially eliminate such risks. An antivirus program, a firewall program and an adware program should be installed on all computers. Such programs are inexpensive but they must be updated on a regular basis to remain effective. Generally, they can be set up to automatically acquire and install updates via the Internet. Virus creators often exploit known software flaws. Microsoft Windows, the operating system used on most computers, is a favorite target. To thwart these individuals, Microsoft makes available free software updates or patches to fix such flaws. Windows can be configured to automatically install these updates via the Internet. Regularly installing the various updates will immunize your computer from most disruptive viruses and software.

Disclosure of client data can occur innocently. Many documents, such as word processing documents, power points and spreadsheets, contain hidden metadata that enables someone reading a file to recover or obtain a substantial amount of hidden data stored in a document. This can include any changes, alterations or deletions, who edited a document and when it was edited. Simple software tools are available to remove all hidden data. Microsoft offers a free removal tool that can be downloaded from its website. Alternatively, files can be transmitted in the common PDF format, which is a graphical format so metadata is not hidden in the document.

Similarly, disposal of old equipment and media can be problematic. Data can be extracted from computer hard drives, disks, tapes and CDs unless they are physically destroyed or subjected to an "erase" program. Unlike the delete function in most software which does not actually eliminate a file, erasing a file makes it extremely difficult, if not impossible, to recover the file.

Traveling with a laptop is convenient but it has some risks. Most public wireless networks do not use encryption or significant security, so data sent over a wireless connection is subject to interception. However, the biggest risk is laptop theft which gives a third party access to any confidential data on the computer. Consequently, one simple way to protect data while traveling is to carry all data on a small keychain hard drive rather than on the laptop. Such drives are small enough to fit in your pocket but they have significant data capacity. The user simply plugs them into a laptop's USB port.

The ubiquity of computers in the workplace coupled with the need to maintain data integrity and block unauthorized access may require hiring technology staff. Most large law firms already employ technology specialists. Medium and small firms may likewise have to hire such personnel. Failure to do so may be considered unreasonable conduct leading to liability in the event confidential client data is disclosed, lost or otherwise compromised.

Attorney and employee education about the risks of using computers plus compliance with a written computer use policy is necessary to protect computerized data. Additionally, is it imperative that complete pre-hire background checks be conducted on all office support personnel. Employee theft of data is a bigger risk than computer hackers gaining access to your digital files.

Exclusive reliance on paper documents could avoid the above concerns. But the use of computers is, and will continue to be, a fact of life in the legal world. Moreover, businesses today rely on computers so attorneys must become educated about the risks associated with computers. Appreciation of these risks enables attorneys to take reasonable steps to preserve client data in accordance with ethical obligations.