Your e-Security Safety Net

How asking the right questions could protect you and your clients

My last column focused on the confidentiality of clients' and attorneys' data or electronically stored information (ESI) as it typically resides in our offices. Those risks haven't gone away: witness the recent news reports that a local attorney lost almost $300,000 because of a sophisticated scam that began when he clicked on a nefarious link to malware. Those risks remain, but there are numerous external risks we confront daily and that implicate our ethical duties to our clients.

The evolution of telecommuting, virtual offices, and mobile workplaces and devices has been rapid. Witness the march of time: the first iPhone (2007); Gmail and Dropbox (2009); the first iPad (2010); and iCloud (2011). These services and devices have facilitated greater information sharing and availability and allowed execution of client tasks from remote locations. Use of these services and devices, however, results in the dispersion of confidential attorney and client information and exposure of that information to additional risks.

As attorneys, we owe the highest duty, and face constant responsibilities, to protect our clients' confidential information and to do so with the ethically-required competence owed our clients. Similarly, we must exert identical efforts to protect our own confidential and proprietary information. The advent of mobile devices, web-hosted e-mail accounts, and remote computing suggests a complexity of execution and security besides what is necessary in a bricks-and-mortar environment.

For instance, we often work at home on client matters. That suggests that our clients' confidential information is resident on our home computers and the mobile devices we use. Some of that information travels on our Wi-Fi networks and is backed up locally or in the cloud. How much protection do we afford that confidential information?

Is our home Wi-Fi network protected by a password? Is its name open to view by anyone else? Is access to it limited only to our particular devices? If we can't answer all these questions affirmatively, then confidential information may be at risk of detection and theft.

Do we share our home computer or iPad with children or with anyone else? Are we certain that others have not downloaded malware that will compromise our data? Do we replicate our office desktop when we're at home? Who else knows the passwords or methods used to access that information?

We should all regularly back up our mobile and home office data. Many of us will use a cloud backup service for that purpose. What do we know about the security of the cloud provider or the location of its site? Can we assume that the provider or the law of its situs will protect our backed-up and confidential information from prying eyes, government subpoenas, or even discovery efforts of litigants with whom we have no relationship?

Nowadays mobile devices enable us to connect with the office or clients from practically any location. If we use public Wi-Fi, do we know whether our communications with clients are encrypted? We should ask the same question if we use anyone else's computer, whether in an Internet café, a hotel, a workplace, or in the home of friends or relatives.

Our mobile devices can hold as much as 128 GB of data. They absolutely require a password or PIN protection if they contain confidential or proprietary information or copies. In addition, if the mobile device is stolen or lost, we must have a method to wipe it clean and protect it from inquisitive eyes. We even have to pay attention to the Bluetooth on our mobile devices that enable functions such as a car phone. Paris Hilton's was left on and enabled, and she lost her entire address book to an electronic snoop.

Current litigation often involves extranets or hosted data locations. What do we really know about the security provided to the confidential information we store and access at those web-based locations?

If we protect information stored at any location with passwords, do we know who else has those passwords? Do we provide them to our accountants? Have we written them down for future reference? Should we be using a password manager? Have we considered two-factor authentication?

The technological changes our profession faces develop constantly, morph frequently, and pose new and complex questions and challenges. We must recognize the changes and prepare to confront them. For instance, Apple's new iOS 8 provides continuity among your computer, your iPhone, and your iPad. You can answer calls on any device. Similarly text messages can be visible on all of them unless you turn off those features.

Walt Kelly's Pogo repeatedly said, "We have met the enemy and he is us." Hopefully he isn't correct.

William Kammer (wkammer@swsslaw.com) is a partner with Solomon Ward Seidenwurm & Smith, LLP.