Don't Be Afraid, Embrace Technology

by Lisa Robertson

A Los Angeles hospital recently made national headlines as the victim of a "malware attack." The information stored within the hospital's computer systems was encrypted and rendered inaccessible to the hospital until a ransom demand was met. (The malware is sometimes called "ransomware.") Reportedly, the hospital received a decryption key after paying a ransom in bitcoins, worth about $17,000. It's unclear to me, from news reports, whether the perpetrators could have viewed or manipulated the information if they wanted to; however, the hospital stated that it found no evidence that any confidential information had been viewed.

Can you imagine losing access to all of your client records?

Law firms across the nation, including in Virginia, have also been targets of these types of attacks, in addition to other viruses and hacking schemes. We understand, in the abstract, that we could be the victims of an attack like this; but, aside from recognizing the risk, are we taking reasonable and proactive steps to protect clients' electronically stored information? As many of you are already aware, effective March 1, 2016, the Virginia Supreme Court amended Rule 1.6, and the comments to Rules 1.1 and 1.6, to provide guidance on the relationship between lawyers' use of technology and their professional obligation to protect clients' confidential information.

In order to maintain the requisite knowledge and skill, "…[**A**] **lawyer should engage in continuing study and education in the areas of practice in which the lawyer is engaged. Attention should be paid to the benefits and risks associated with relevant technology.**" *See* Rule 1.1 (Professional Competence), revised comment [6]. This comment encourages us to embrace technology, rather than avoid it, and to consider new practices that will enhance the quality of legal services — even if we're afraid of them. What constitutes "relevant technology" in your practice? In my own experience, technology relevant to my practice has included: copy machines that store information from scanned documents, faxes and e-mails; phones and tablets used to send, receive and store electronic information; VoIP[1] telephones and voice mail; desktop and laptop computers; data storage devices—floppy disks, CDs, external drives, and the Cloud; and various software, "apps," operating systems, and internet services that allow document sharing, calendar management, client communications; client payments; and banking, payroll and accounting functions.

Most of us utilize some combination of the technologies listed above. Fewer of us understand how they work, or understand the various ways in which our own patterns of use can make the devices we use to communicate with clients, or to store their confidential information, vulnerable to viruses and hacking, or even to unauthorized access within our firms. To assess the risks of a particular device or application, one needs to have some familiarity with its functionality, or the means to hire an employee or consultant who does. Luckily, I work in a setting that employs a department of IT professionals, but I still worry about how to satisfy my professional obligations through my own daily practices, and about the cost to my employer/organizational client of implementing security measures.

Under the new provisions of Rule 1.6, every lawyer is required to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, confidential information. *See* Rule 1.6(d) and Comment [18]. In revised Comment [20] to Rule 1.6, the Supreme Court has indicated that reasonable efforts are satisfied by a lawyer or law firm that employs:

> "…**appropriate data protection** measures for **any devices used to communicate or store client confidential information**…. Because threats and technology both change, lawyers should periodically review both and enhance their security as needed; steps that are reasonable measures when adopted may become outdated as well…." [***Emphasis added***]

Does my office copy machine store copies of scanned e-mailed or faxed documents? Where and for how long will information reside on the copier, and how can it be protected from unauthorized access? If my smart phone is lost or stolen, how do I remotely wipe its memory? Is that the best thing to do? What malware protection is available for a smart phone? When information is stored in the Cloud, where does it actually, physically, reside? How do I verify that the information is safe at that location?

I and the other members of VSB's Special Committee on Technology and the Practice of Law are working to promote greater access to resources that can help Virginia lawyers identify and manage the risks of technology, and to embrace the great client service and practice management benefits that technology can offer. We encourage local bar associations and specialized associations to include technology education components in their CLEs. We also hope that you will consider attending

Technology *continued on page 50*

Technology *continued from page 48*

the Virginia State Bar's upcoming TECHSHOW (April 25, 2016, at the Richmond Convention Center). The TECHSHOW provides a unique opportunity for lawyers to simultaneously discuss the latest technology, how to use it, and how to protect information. We want all of you to be contemplating these interesting and challenging issues.

Endnotes:

1 Voice Over Internet Protocol (VoIP)

Lisa Robertson is the chief deputy city attorney for the City of Charlottesville. She is a co-chair of the Virginia State Bar's Special Committee on Technology and the Practice of Law. Her practice includes all aspects of local government operations and administration, including public record-keeping requirements.