2017: The Year for Encryption

Add another necessary layer of protection this year — encryption

We know that we owe our clients a duty of confidentiality, and we also want to ensure the confidentiality of the details of our practices and our finances. But the duty we owe to our clients goes far beyond the principles of the attorney-client privilege. The State Bar Act codifies our duty of confidentiality by telling us we must "maintain inviolate the confidence, and at every peril to himself or herself, […] preserve the secrets of his or her client." Cases and opinions teach us that the Act requires diligent protection broader than that of the privilege.

About ten years ago, the various ethics committees began their efforts to apply these confidentiality principles to the modern methods of communication and technology that were impacting and altering our law practices. California addressed electronic methods of communications in 2010, and, more recently in 2015, our duties of technology competence.

> "No matter the technology firewalls and boundaries, human error will still account for 80-90% of successful intrusions."

We must be aware of the cybersecurity risks faced by lawyers and their firms. Recent headlines reported the indictment of Chinese hackers who had penetrated the electronic systems of several prominent law firms (Cravath; Weil Gotshal) to obtain information that allowed them to take financial advantage of pending transactions. A recent American Bar Association report found that 90% of their IT respondents reported that their organizations had experienced a breach of document security in a particular year.

Preventing the invasion of our electronic systems will continue to be a problem because, no matter the technology firewalls and boundaries, human error will still account for 80-90% of successful intrusions. Walt Kelly's comic character Pogo used to say, "We have met the enemy and he is us." Because of that inevitability, we must establish a second defense layer that prevents the intruder from obtaining unauthorized or inadvertent disclosure of or access to client confidential information. Erecting firewalls and posting cybersecurity checkpoints has become insufficient protection. Encrypting the contents of the information that lawyers hold should be the new confidentiality requirement going forward into 2017.

Encryption converts information and data into forms unreadable by anyone other than an intended recipient or an authorized individual. Encryption is not a new technique; some historians recite a first use by an Egyptian scribe around 1900 BC. Cryptanalysis dates back about 100 years, and the military has used complex encryption for the past 75 years.

Most of us know of the need to protect communications in transit and when using public Wi-Fi networks. We should already know how to encrypt our emails and the Office documents we send as attachments. We can also encrypt the information we send over the internet. In 2010, a California opinion (2010-179) stated that the encryption of email "may be a reasonable step" for attorneys. Some would now assert that it is a necessary step.

What has now become equally important is the encryption "in place" of the information resident on our servers, desktops, laptops and mobile devices. In 2014, a local attorney left his laptop on the trolley, and the result was a data breach requiring the expensive process of notice to clients, not to mention the public embarrassment. The data on the laptop was not encrypted. We can't assume that we are incapable of a similar mistake with a laptop or mobile device. TSA recently reported that 70 laptops had been left at TSA checkpoints in Newark Airport in the

Continue on page 38