iWitness

HOW ONE FIRM UPGRADED SECURITY

WILLIAM M. LOW

The author is a partner at Higgs Fletcher & Mack, San Diego.

Change can be difficult and challenging, especially for lawyers. Over the past year or so, my law firm has made a concerted effort to improve our cybersecurity defenses. The process is ongoing, and we still have a lot of work to do. Despite the occasional aggravation, I think the results justify the time and effort we've put in. There are three major areas we needed to think about: (1) individual employee conduct, (2) central office systems security, and (3) using the cloud.

First, the "easy stuff," which, perversely, caused much of the aggravation. I'm referring to implementing basic security principles, including workstation lockout, password security, and portable storage protocols.

The Easy Stuff

Workstation lockout is familiar to anyone worried about battery life on a laptop. How long do you wait before an unattended workstation signs off and forces you to reenter your password ? Hyper-vigilant security experts might say "30 seconds," while senior partners who enjoy getting up from their desks to walk down the hall to talk to a colleague could easily say "three hours" or "all day." This isn't a casual issue. While in the office on weekends, I regularly saw workstations that had been left on since Friday. Leaving your system open to random examination—or worse—by janitorial staff, building maintenance workers, clients, or other lawyers with their clients is obviously unacceptable. As a fair compromise, we settled on 20 minutes of no activity before lockout. After all, how burdensome is it to reenter your password after you get back from lunch?

That brings us to passwords—the subject of some of the loudest pushback. You know the arguments: Not changing your password is an invitation to sharing or theft, while always changing your password leads to forgetting it and to the ubiquitous "Post-it note password system." Try it. I dare you. Walk around your office and see how many Post-its with passwords you find on screens or tucked beneath keyboards. So we bit the bullet and required that every user's password be at least eight characters in length, with both uppercase and lowercase letters, and at least one number or symbol. To make matters "worse" (from the users' vantage), the network itself forces a change of individual passwords at least every 90 days. This is, without a doubt, a pain and has generated a lot of complaints, especially because the system doesn't allow users to simply recycle old passwords.

The last "simple" security issue was another big favorite in the office—deactivating all workstation USB drives. This provoked anguished cries from several of our lawyers, who claimed they couldn't function without their thumb drives. I'll be the first to admit that USB thumb drives are an incredibly simple, easy, and convenient way to transfer large amounts of data. I had become used to copying file materials and deposition transcripts and exhibits onto a thumb drive when I traveled.

Similarly, clients would often give me thumb drives full of materials I could take back, plug in, and copy onto our system. A thumb drive retailing today for about $10 can carry more text than is generated by most cases. But we decided the convenience of using the thumb drives is far outweighed by the risks.

Risks? There are several. First, hackers are using USB thumb drives to transmit computer viruses and malware (think Stuxnet). When a client hands you a thumb drive, no matter how much you may trust the client, you have no way of knowing where that thumb drive has been or what virus- or malware-infested computer it was previously plugged into. Also, hackers have been known to "seed" the parking lots of businesses they're trying to break into with USB thumb drives

Published in *Litigation*, Volume 41, Number 4, Summer 2015.

carrying malware, successfully betting that curious employees would pick up and use the drives at work. Finally, because they are so small and capacious, they are ideal for a thief or a disgruntled, soon-to-be-former employee to walk critical information past the front desk.

We decided to deactivate all USB drives on all workstations except those in our information technology (IT) department. (We briefly considered, but rejected, the U.S. Army's preferred method: glue in the USB ports.) As a result, the IT department has become the clearing house for all portable storage devices. They first scan inbound drives for viruses and malware before uploading the data to the network. Similarly, if a lawyer is traveling and needs to copy files onto a thumb drive, he or she has to advise IT in advance which files need to be transferred to the thumb drive and get the thumb drive from our IT department. What happens if the thumb drive is lost or stolen? All of our thumb drives are now encrypted. If a lawyer needs to transport really large amounts of data, we have encrypted portable hard drives that self-wipe after a certain number of failed attempts to open them without a valid password. (I was in favor of the James Bond–like exploding security feature but was outvoted.)

Illustration by Lisa Haney

As far as moving large blocks of data to trusted third parties, however, we've found an easier way that eliminates the IT bottleneck. Using a third-party provider like Citrix or Mimecast, we now can securely send a relatively large volume of records and files to clients or experts over the Internet. Here's how it works. Let's say I have medical records I want to send to an expert witness for review. Using this system, I can sit at my desk, create an email, select from our network which files I need to send, and then send them to my expert through the third-party provider. Rather than traveling over the Internet like a customary email, my email and the files are sent securely through a VPN tunnel directly to the third-party provider, which, in turn, sends my expert a link to the files. (A VPN, or virtual private network, is essentially an encrypted channel through which you can securely communicate via the Internet without your message being seen by others.) The expert clicks on the link and is then separately sent a password to access the files. The files are sent directly to the expert. The link remains open for only a few days; if the expert doesn't promptly use it to access the records, it dies and I would have to resend the files. I also can arrange to be notified electronically when the link has been activated and the files have been downloaded.

One important thing to keep in mind when considering whether to send confidential files via a USB thumb drive rather than securely over the Internet is that, so long as the files remain on the encrypted thumb drive, they will remain encrypted. If the thumb drive is lost or stolen, you won't need to worry (much) because it is encrypted. But if you send records and files securely over the Internet, once your client or expert downloads them onto his or her computer, they cease to be encrypted. If that laptop goes missing or is stolen, that could be a problem. Your client or expert should know this and take appropriate steps to protect and secure his or her laptop or workstation.

Smart Phones

This brings us to smart phones. Our lawyers use their smart phones to access firm email. When properly set up to access our network, the personal smart phones become "trusted devices" as far as our network is concerned. From our network's perspective, this means the device can communicate directly with our network and be used to send and receive files with nary a second glance from our firewall and network perimeter defenses. So if I use my personal smart phone to go online and then click on a link that downloads malware onto my phone, the next time I use my phone to check my email, that virus conceivably could get past our firewall and antivirus systems and into our network. More commonly, this happens when you give your phone to your child to let her play with apps and she downloads something nasty. Or you lose your phone without it being password-locked and a bad guy uses it to access your firm's network. Either way, a potential intrusion.

We saw the use of personal smart phones—known as BYOD (bring your own device)—as a serious risk to the firm network and our client files. We decided that only firm-issued smart phones would be able to access our firm network. The phones are password-protected and can be erased remotely if they go missing or are stolen. They lock out after several minutes of inactivity, and the password feature cannot be deactivated without automatically wiping the phone. Finally, the smart phones can be set up to segregate personal data from firm data, and we can remotely wipe the entire phone or only the firm data. Not surprisingly, eliminating the BYOD regime has generated some pushback from our lawyers, who don't like the idea of having to carry around two smart phones, one for work and one for home. So we decided to allow our lawyers to use firm-issued phones for personal use as well as work. We feel that the "keep your work and private data separate" technology discussed above, plus allowing employees to copy their private data in a reasonable time if they leave or are terminated, fairly addresses these concerns.

> The weakest link in your cyber defenses will always be human—your attorneys and staff.

Also, we have improved our network infrastructure, including upgrading our firewalls and antivirus software, using a fairly aggressive spam filter, and regularly scanning for junk email, phishing attempts, and potentially infected attachments. In this regard, we had some very useful suggestions from our cybersecurity insurance carrier. If you don't yet have cyber insurance, I strongly encourage you to do so. Meeting with your cyber insurance reps will be an eye-opening experience.

To make sure our firm is equipped to handle the unthinkable—a devastating fire or earthquake that destroys our computer servers—we made the decision to migrate our servers into the cloud. We investigated a number of cloud providers based in the United States. Among other protections, we made sure our cloud provider is required to preserve the confidentiality and security of our data, uses technology to protect against "reasonably foreseeable" attempts to improperly access the data, and is required to notify us if subpoenaed or otherwise asked to produce our data to a third party. As an added safeguard, we separately contracted with a third party that handles the administration of the cloud system and encrypts our data *before* the data reach the cloud provider's servers. We alone hold the encryption key. Finally, our encrypted data are housed in more than one location by our cloud provider so that if one cloud location goes down or has a problem, another seamlessly steps in.

The most difficult task has been, and will continue to be, the training of our attorneys and staff to "practice safe cybersecurity." While no cybersecurity defense can realistically be expected to be 100 percent effective, the key is to use layers. The weakest link in your cyber defenses will always be human—your attorneys and staff. As a result, we have started to train our employees to be aware of spearphishing forays and social engineering, and to "think before you click" on email links or attachments. We know that the training of our lawyers and staff will present the greatest challenge and likely will be a never-ending process, as the bad guys of the world continue to devise new and ingenious ways of attempting to steal our clients' confidential information through cyberspace. ■