It's About the Money — Cyber Attacks

by Frances Lynch, Esq.

Frances Lynch is a partner in the law firm Bache & Lynch. She is a trial attorney and graduate of the nationally known Trial Lawyers College. In the course of her career, she has had numerous jury trials, and has successfully represented people in many communities and courtrooms throughout Arizona. She has devoted her career to protecting the rights of people and to educating non-lawyers about the judicial system

Frances is a strong believer in taking the time to educate clients about their legal rights. She has taught Media Law at the University of Arizona Journalism College, is the author of the book *Draw The Line: Guide to A Sexual Harassment Free Workplace*, (Oasis Press 1995), is a contributing author to *World of Criminal Justice* (2001), *Encyclopedia of Everyday Law* (2002), *Notable Black American Women* (2002), and *West's Encyclopedia of American Law* (2004), all published by The Gale Group.

Frances has spoken and taught Continuing Legal Education at the local and state level for Arizona Association of Justice. She has always been an early adopter of technology and incorporates it successfully into her practice on a daily basis. Frances' practice is devoted to serious personal injury and wrongful death cases.

Technology may have made our lives easier in many ways, but right now, attorneys are targets for financial cybercrime. As reported by the American Bar Association (ABA) last year, even small law firms are now under attack, targeted by cyber criminals. According to an ABA report, about 27 percent of firms with two to nine attorneys reported experiencing some sort of security breach. According to a recent ABA survey, 15% of all law firms have fallen victim to a breach. This is not an anomaly. And there is no shortage of horror stories.

Last year, Attorney Doe[1] who is an extremely experienced Arizona attorney and a frequent speaker on wrongful death and personal injury, settled a catastrophic injury case for a large sum of money. This was not unusual for Doe. What was slightly unusual about this case was that Doe had co-counsel in another state. It was agreed that Doe would receive, deposit and disburse the settlement funds. When the time came to disburse funds, Doe emailed out of state co-counsel about how to disburse, and got an email response directing Doe to wire transfer the out of state firm's share of the fees and costs. The email was from a paralegal Doe had been communicating with all along, and stated that the firm had a problem with their trust account so Doe was going to need to wire transfer to a new account the firm had set up. The email address appeared to be the correct email (although Doe would later notice that the address was missing an "s" letter in one of the names.)

Doe made preparations to wire transfer the funds, which were substantial, and received at least two more emails from the paralegal relating to the transfer. While thinking about it, Doe became suspicious, not because of the emails, but because of the "other" account. Doe picked up the phone and called co-counsel's paralegal. Doe explained the concern about the "other" account only to learn ***the paralegal had no idea what Doe was talking about*** and had never received Doe's initial email about disbursing funds. Doe mailed a check and avoided a disaster. Hackers were apparently monitoring the email account of co-counsel, and tried, unsuccessfully, to intercept the funds by tricking Attorney Doe.

Often, the goal of hackers in not to steal law firm files. Instead, the hacker threatens the electronic "key" to unlock the encrypted files will be destroyed, rendering the hijacked files forever inaccessible. This is known as "Ransomware." An email demanding the ransom may show a digital clock that counts the minutes and seconds to the deadline. When the timer expires, the ransom demand goes up until the victim pays. If the victim doesn't pay, the data is permanently locked and unrecoverable.

A lawyer in upstate New York unwittingly opened an email attachment that he thought was from someone he knew. It was actually part of a phishing scam. In a phishing scam, a hacker often poses as a colleague in an attempt to retrieve the victim's personal data. Most of the time, this comes in the form of an email that appears to be from a legitimate entity, but is not. When the New York lawyer opened the attachment in the phishing email, it immediately locked down the law firm's network. The data was encrypted by the hackers who demanded $24,000 for return of the firm's data.

Ransomware enters a system in several ways: an unsuspecting user clicks on email links in phishing scams, a user visits fraudulent or unsafe websites, or a user inserts an infected USB drive. The ransomware then encrypts all the user's files and folders. It can propagate to data in the entire workplace through the existing network. Restoring data from backups is often the only way to retrieve data. The last backup is often what is left, so it is crucial that backups work well and work often. If no backup exists, the only solution is to negotiate and pay the hackers for the key to the encryption lock. Paying the hackers is of course the equivalent of negotiating with terrorists and rewards those perpetrating the crime. Nevertheless, in at the New York law firm, perhaps because the lawyers were experienced negotiators, the partners ended up paying $5,000 (rather than $24,000) for their own data, and another $15,000 for information technology advice and new equipment. The firm had purchased cybersecurity insurance, and the insurance company paid the claim.[2]

Keep in mind that phishing emails could fraudulently appear to be from someone known, such as opposing counsel, co-counsel, a bank, an employee, or an email provider. Often these emails ask the recipient to click on a link or to confirm certain personal information. Phishing scams are complex and can link to fake web sites and phone numbers which appear legitimate.

Learning about cybercrime risks is not just good business practice. The Arizona State Bar expects it. The comments to E.R 1.1 under Maintaining Competence[3] provide that "[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice***, including the benefits and risks associated with relevant technology***."[4] Of course, an insurance policy which covers cyber security breaches may also prove useful. And when in doubt, don't hesitate to pick up the phone and communicate the old fashioned way. Even the most astute of us can be deceived.[5] ■

ENDNOTES

1 The attorney's name is fictitious to protect client confidentiality; the events are factual.
2 http://www.abajournal.com/magazine/article/biggest_cybercrime_risks_lawyers
3 https://www.azbar.org/Ethics/RulesofProfessionalConduct/ViewRule?id=3
4 Id.
5 For more on this concept see Gladwell, Malcolm Talking to Strangers, Little Brown, 2019.