1. Cybersecurity

ABA Formal Opinion 477R,
Securing Communication of Protected Client Information (May 19. 2017), available at
https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-477.pdf

ABA Formal Opinion 482,
Ethical Obligations Related to Disasters (Sept. 19, 2018), available at
https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-482.pdf

ABA Formal Opinion 483,
Lawyers' Obligations After an Electronic Data Breach or Cyberattack (Oct. 17, 2018), available at

https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-op-483.pdf

*Published in **Law Practice***
(September/October 2021
by the American Bar Association.

ETHICS

Our Ethics Duty to Read the News

By Lucian T. Pera

As lawyers, we have an ethics obligation to keep up with news of the latest cybersecurity disasters. And ask our personal tech guru questions about what they mean for us.

Turning to the Rules

As we ethics nerds often do, let's start with the ABA Model Rules of Professional Conduct.

Rule 1.1 requires that we provide clients competent representation, defined as "requir[ing] the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." In an overwhelming majority of jurisdictions, the Comment to the Rule provides 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. . . "

In plainer English, we need to know how to effectively and safely use the technology tools necessary for our work, and we need to keep our knowledge and training on this score updated.

The confidentiality rule agrees. Rule 1.6(c), also adopted in an overwhelming majority of jurisdictions, requires us to use "reasonable efforts" to keep client confidential information secure from unauthorized disclosure, whether inadvertent or nefarious. The Rule's Comment lays out a series of common-sense factors that we must use to evaluate what amounts to a "reasonable effort," and ABA Formal Opinion 477R gives us a nice primer on those factors.

ABA Opinion 483 teaches not only what we're ethically required to do to respond to data breaches and incidents, but also makes the obvious point that we're ethically required to make reasonable efforts to protect against such threats to the sanctity of client confidential information.

Discipline for Skipping the News?

Sure, you say, but where do the rules say a lawyer is going to get disciplined for not reading the *New York Times* for the latest on big hacks?

OK, so maybe I overstated a bit. But you're still reading. And my point is simple, if not as threatening: By reading the headlines about notable hacks and cybersecurity threats, plus just a wee bit more, you can be safer and more knowledgeable about the risks to you and your clients.

Enter Your Tech Guru

For years now, I've preached that, in these technologically dangerous times, every lawyer needs a tech guru, whether inside your firm or a cell phone call away.

That's the reliable, pre-vetted person who takes care of your IT needs. They help design your systems and pick your tech. They answer your routine tech questions. And they will answer the phone on Saturday night at 9:30 when you panic when someone steals your laptop from your car while you and your spouse were at dinner.

My pitch: As lawyers, we need to be alert to the news of hacks and cybersecurity incidents, whether specifically about lawyers or not, and we should have regular conversations with our tech guru about them. They can be teachable moments. We need to train ourselves to be in regular learning mode. Because we can learn from others' experiences and mistakes.

Two Questions for Your Tech Guru

The next time you read a story of a big tech security disaster, consider asking your tech guru two questions about it: First, am I safe from this particular danger? Second, is there anything I can learn from it?

Two Examples

Over the last year, two big teachable moments come to mind: the SolarWinds data breach and the Microsoft Exchange server hack.

SolarWinds

In December 2020 and early 2021, the world learned that a bad international actor—most probably Russian government-backed—had severely compromised software sold by Texas-based company SolarWinds. This Orion software is used in the background of company networks to manage IT systems. About 18,000 SolarWinds customers used this well-regarded software.

The bad guys secretly loaded malware into the Orion software. That allowed the malware to enter the networks of SolarWinds customers undetected—after all, the software was from a trusted source. The malware then took up residence in

those customer networks and gave the bad guys unauthorized access to the customers' networks.

Eventually, at least one prominent cybersecurity company and numerous federal government agencies were attacked. Cybersecurity firm FireEye was a victim, and some of its own tools for investigating breaches were stolen. The U.S. Department of Justice was attacked and about 3 percent or 3,450 Microsoft 365 mailboxes were potentially breached. The attacks also reached federal court computer systems, including their CM/ECF filing and case management systems. (The new restrictions on how particularly sensitive documents are filed in federal court are a direct response.)

Asking the Tech Guru

When you talked with your tech guru, here's what they might have said.

First, am I safe from this particular danger? If your firm or law department doesn't use the Orion platform, then probably so.

Second, is there anything I can learn from it? One moral is that we're all vulnerable to hacks of our trusted suppliers—"supply-chain attacks." We need to vet suppliers, but, in this instance, SolarWinds was well-regarded, with little to alert its customers to their vulnerability. At some point, you and your tech guru must have some vetted, trusted suppliers, and live with some level of risk.

There are things your tech guru may have learned—things normally beyond a lawyer's tech ken—that may protect you. Knowing that your tech guru is in constant learning mode is always reassuring.

For example, FireEye discovered a device registered to their system that was not actually used by an employee. Systems can set to check and alert whether devices are accessing the network that shouldn't. Even a cybersecurity firm's defenses were not perfect. Also, there may be "endpoint" protection software that would detect signals that malware had creeped in through a trusted supplier. And experts insist that many network devices and software have logging capability that not all users enable. Maybe they should.

The Microsoft Exchange Server Hack

The media extensively reported the SolarWinds attack. Somewhat remarkably, however, there seemed less reporting of the Chinese government–based attack on several vulnerabilities in the software that runs Microsoft Exchange servers.

The world learned in early March 2021 that the bad guys apparently found several vulnerabilities in Exchange server software. That software powers every

Microsoft email system, other than those run on their online service, Microsoft 365. About a week after Microsoft's announcement and patch release, one security company reported finding more than 99,000 servers online running the software unpatched.

Initial reports were that at least 30,000 U.S. organizations, including more than 4,000 state and local governments and infrastructure providers, had been hacked as a result.

Microsoft quickly developed a patch and pushed it out to users. Of course, Microsoft also quickly patched its own servers running Microsoft 365. Microsoft released patches for versions of the server software dating back to 2010.

Asking the Tech Guru

What might your Tech Guru have told you had you asked?

First, am I safe from this particular danger? If your email comes through your own Exchange server, it had to be patched and checked for evidence of hackingimmediately, for you to be safe. With luck, your tech guru would have said, "It's patched, and I checked it, and we're safe."

If your email is provided through some server other than your own Exchange server—either through Microsoft 365 or some other non-Microsoft service—you're in the clear.

Second, is there anything I can learn from it? Yes, the big lesson concerns the difficulty of handling your own IT security and the value of the cloud.

Those who own their servers had to patch them instantly, and then check and secure them. Subscribers to Microsoft 365 had outsourced their security and could, quite reasonably, expect that Microsoft would patch its own servers, and protect all its users, at least no later than the released of its patch to Exchange server owners.

I read this as a testimonial to the likely greater security of (carefully) outsourced IT security and, more generally, the cloud.

Put another way, when your tech guru told you this, you might have asked, "So why are we still running our own server?"

Our ethical obligations amidst the dangerous tech environment in which we find ourselves demand that we stay informed about new threats and how we are positioned to protect ourselves. Having a nice water-cooler chat with our tech guru about the hacking news of the day just might help you do that.

Lucian T. Pera is a partner in the Memphis, Tennessee, office of Adams and Reese

LLP. He counsels lawyers, law firms, clients and those who do business with lawyers and law firms on ethics and professional responsibility issues. He's a past President of the Tennessee Bar Association and a past ABA treasurer. Lucian.Pera@arlaw.com.