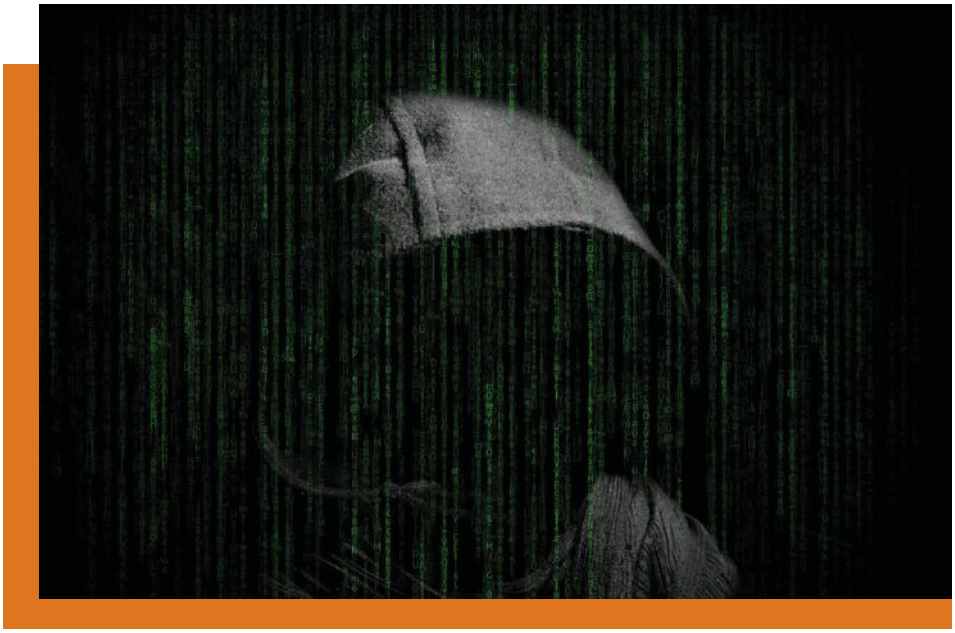
By DANIEL J. SIEGEL

Preparing for the Dangers of the Online World

Face it—whether you are young or old, techie or Luddite, or just want to cling to the ways of the world as it was decades ago—there is a lot of scary tech news out there. And for those who claim that they want to return to the days before the Internet, consider the following list:

- Smartphones (or even flip-phones)
- Google
- GPS systems, Google Maps, and MapQuest
- MP3s, iPods, and iPads
- E-filing
- Kindles
- Wi-Fi



None of these things existed 30 years ago when the Internet started to be a "thing," and many did not exist as recently as 10 years ago. How many of us would want to return to those days? Even if you do, you can't.

Which means you need to recognize the risks and benefits of technology as they relate to your law practice. Oh yeah, that phrase was not part of an attorney's duty of competence until its inclusion in the Model Rules of Professional Conduct in 2012.

It can be a scary world out there. Consider two events that happened to Philadelphia lawyers in the past year. One lawyer, who handles estate administration, received a call from a client who had received an email "from the attorney" with instructions to wire funds to pay inheritance tax. The email looked like it came from the attorney, but it did not. It came from a hacker who spoofed the attorney's email and made a copy so realistic it was virtually impossible for anyone, let alone a less than tech-savvy client, to recognize that it was not real. The client wired the money, as instructed, and received a second similar email, and was going to follow the instructions when she finally decided to call the attorney. It was then that she learned that the emails were bogus. But not before she had transferred more than $20,000, and her money was gone.

Would you want to be that attorney? Would you want to have to explain to your client that she was bilked? What is the attorney's liability, if any? What are the chances the client changes lawyers?

In another instance, a regional law firm that represents insurers in personal injury claims against its insureds learned that a hacker had accessed its cloud-based backups, including the records of countless plaintiffs from numerous states. The hacker had access to the personal information of every plaintiff whose information was stored on the site, all because of a programing error.

Would you want to be that attorney? Would you want to tell the carriers you represent about the hacking? And would you want to tell the individual plaintiffs (and their counsel) about the hacking?

In each instance, can you picture the client firing the attorney or firm?

And, of course, consider the publicity that would result if the firms' identities became public. Contrary to the old maxim, not all publicity is good publicity.

These were not highly complex incidents, at least not from the lawyers' or law firms' perspectives. Each was preventable or, at the least, could have been averted with a bit more diligence.

Lawyers are easy targets for cybercriminals. Every time I write or lecture, or speak with lawyer/victims, I hear the same retort, "I never thought it would happen to me." It does, and it will.

Why are lawyers easy targets? Because most are either deniers who do not believe "it" can happen to them or are those who hear the warnings and do nothing. Only a few firms are proactively secure. Most allow me to scare them—at seminars, in my columns, and during consultations—and then go back to business as usual. And everyone (including hackers and criminals) knows that lawyers have access to, and maintain, sensitive information about their clients.

It's time for those lawyers to stop being scared and to do something. So, what steps should lawyers and their firms take to protect against cyberattacks? Here is my seven-step plan:

Firms should know and control the information to which each employee has access, and also whether the data, including information stored on smartphones and other mobile devices, is encrypted and password protected.

1. Analyze Your Firm's Current Status

Every firm should perform a cyber-assessment and inventory of all hardware, software, data, and other technology. Create an inventory of all computers, servers, printers, mobile devices, and other "things," such as flash drives, etc. Having this information will enable the firm to see whether any hardware is outdated, unprotected, or otherwise a security risk. Next, do the same for software. Having information, such as passwords, licenses, and versions, will help assess whether any software is no longer supported or otherwise vulnerable. Firms should also identify all stored data and where it is stored, who created it, and with whom it is shared.

Not only will this information help assess and pinpoint any security deficiencies, it will also facilitate creation of a long-term plan for replacement of outdated technology.

2. Evaluate Your Cybersecurity Systems

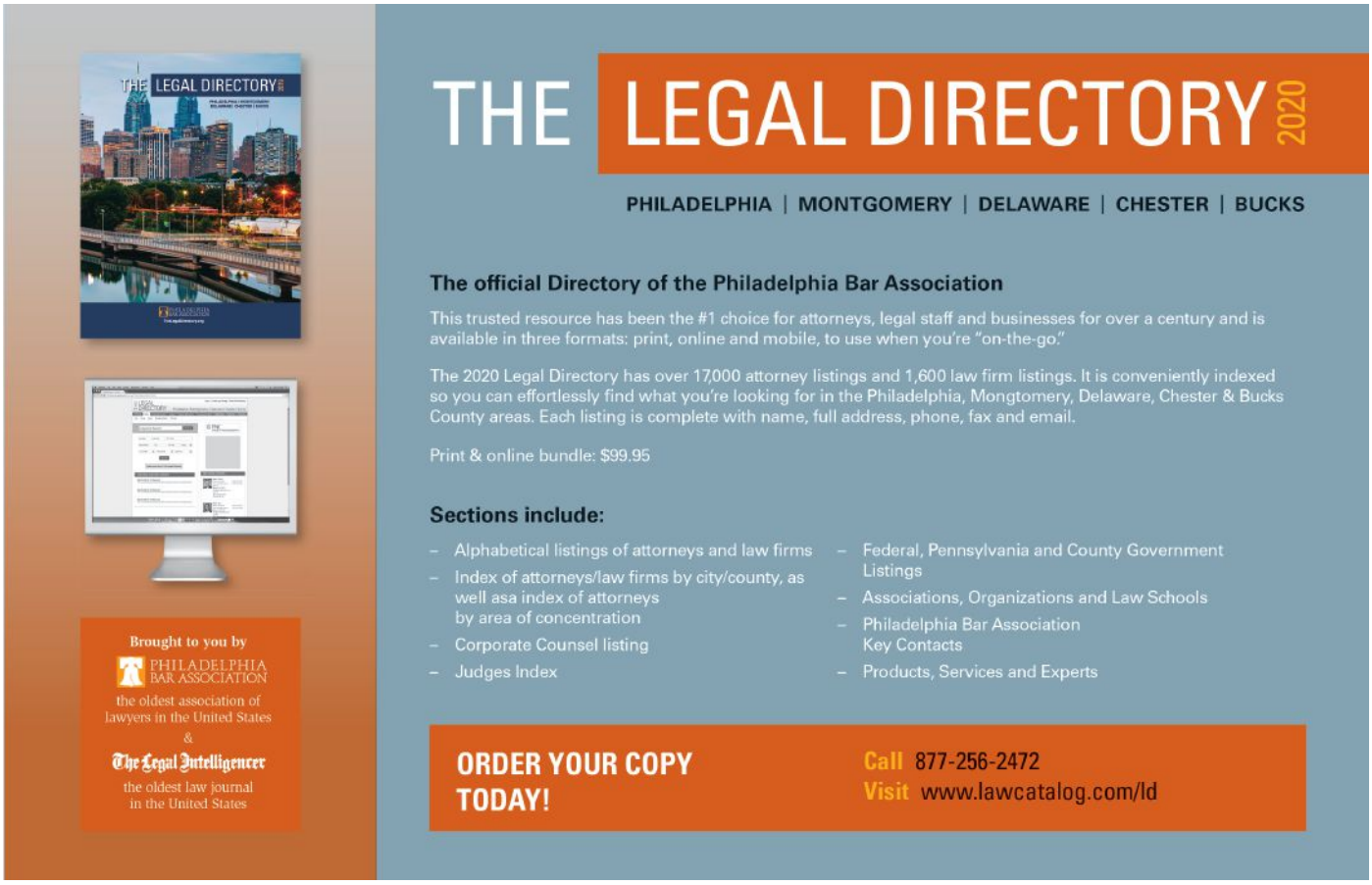
This step is crucial. Firms should know and control the information to which each employee has access, and also whether the data, including information stored on smartphones and other mobile devices, is encrypted and password protected. There should also be a record of all passwords for all devices. Finally, the firm should verify that it uses up-to-date antivirus, anti-malware, and firewalls.

3. Employ Basic Technology to Prevent a Cyberattack

Everything need not be complicated. Most vulnerabilities are the most obvious. Firms should have spam filters, anti-malware, antivirus and anti-spyware software, as well as hardware- and software-based firewalls. In addition, staff using mobile devices (isn't that everyone?) should be required to connect their devices through a VPN.

4. Evaluate Your Vendors' Security

This is a scary prospect for many firms. When necessary, call in a consultant. But at a minimum, require vendors to show their security



[Cyberattacks] happen to companies like Target and Wawa, and can easily target lawyers, courts, and others whose infrastructure is inadequate

certificates. If you don't know what I mean, hire or use a consultant.

5. Create Policies and Procedures

Many law firms do not have technology-related policies, including those for cybersecurity, email security, web access and usage, firm technology, and for staff-owned devices. There should be policies in place, and every staff member should be required to acknowledge that they have read and will comply with these policies.

6. Train Employees – New and Old

Training is essential—for all employees—so that everyone is aware and acknowledges their obligations toward technology policies and procedures. Staff should be trained to recognize dangers, and the firm should adopt policies through which staff can preemptively discover and respond to inevitable dangers.

7. Purchase Cyber Insurance

Cyber insurance has become a necessity for law offices. In most cases, a "rider" to a general liability insurance policy will not provide enough protection for the many dangers that confront firms. Rather, because cyber-dangers are a "when" not an "if" concern, having appropriate cyber insurance should be mandatory. These policies protect against a wide range of dangers, and generally cover the costs of hiring consultants, new equipment, marketing, and other associated expenses. Without appropriate insurance, firms run the risk of financial ruin if a cyberattack is sufficiently robust.

Cyberattacks will happen. They do every day. They happen to companies like Target and Wawa, and can easily target lawyers, courts, and others whose infrastructure is inadequate. As we venture into the third decade of the 21st century, law firms must finally be proactive in preparing for and responding to the inevitable threats and dangers that they will confront. ■

When You Need

- Social Media Searches
- Scene/Vehicle Photos
- Motor Vehicle Searches
- Asset Searches
- Surveillance
- Process/Courier Services
- Background Checks
- Employee Terminations
- Pre-Employment Searches
- Witness Statements
- Litigation Support
- Product Liability Investigations
- Record Searches/Procurement
- Mobile Notary (In some locations)
- Skip Tracing
- Insurance Investigations
- Medical Malpractice Investigations
- And Much More!

You Need...

HARRIS INVESTIGATIONS

LARGE ENOUGH TO SERVE, YET SMALL ENOUGH TO CARE

Covering PA, NJ, DE, MD & WV

Servicing Attorneys, Businesses, Insurance Carriers & Individuals

Pennsylvania: Lansdale, Norristown, Bethlehem, Boyertown, Pine Grove, Uniontown, Harrisburg & Pittsburgh

New Jersey: Lawrenceville & Elmer **Delaware:** Wilmington & Lewes

www.HarrisInvestigations.net | (888) 484-9827 | Harrisinvestigationsllc@yahoo.com

CONTINUING LEGAL
EDUCATION
PHILADELPHIA BAR ASSOCIATION

The Philadelphia Bar Association offers webcasting of its CLE programming.

For course offerings and to register, visit the CLE page at www.philadelphiabar.org.