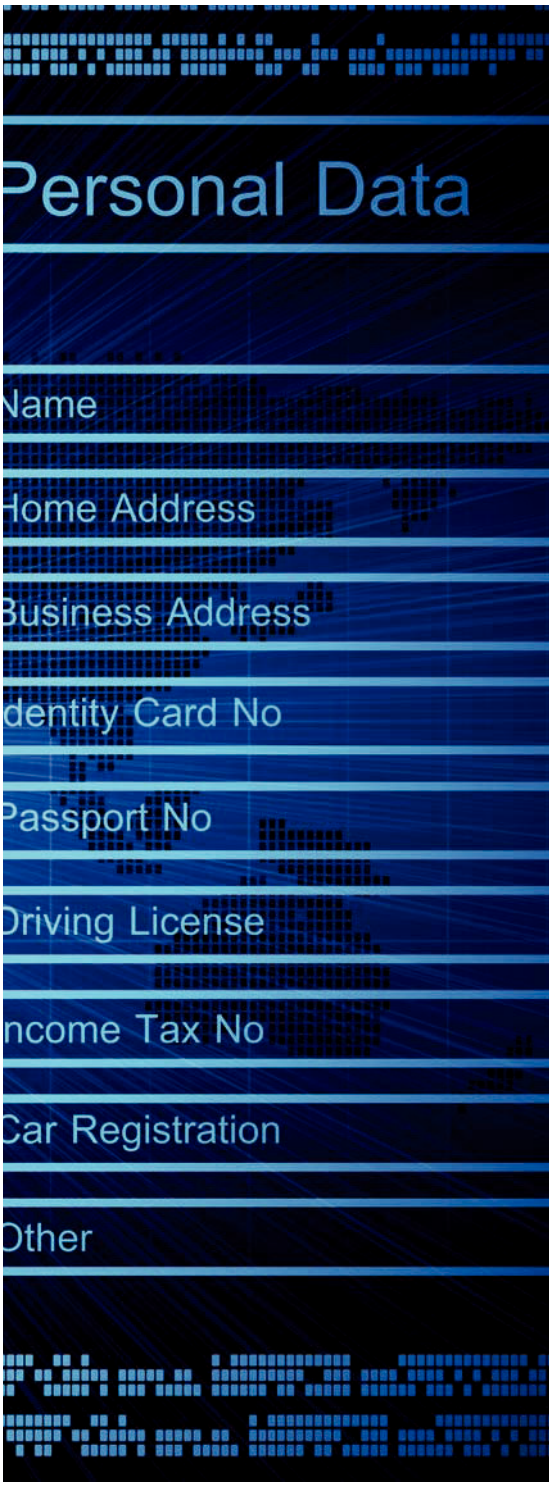
CYBERCRIME AND FRAUD YOUR HOME, OFFICE, AND

iStock

PREVENTION FOR CLIENTS



Solo and small law firm practitioners are in an excellent position to take charge of their own technology, cybersecurity, and fraud prevention while simultaneously gaining practical, hands-on knowledge. The scale of our computer systems is much smaller than that of larger firms and corporations, which makes it worthwhile for us to take the time to learn about them. A sole practitioner's computer system at work may be similar to a home system, so if we invest the time to learn about and secure our homes and family—and we should all want to do that—then we will have learned enough to secure our workplace, too. Often the solo and small law firm practitioner acts as the IT department and is the first to experience issues, troubleshoot, and either fix them or communicate about them to an outside IT firm.

Some cybersecurity guidance can seem overwhelming, and technology can often seem like a mystery. Fortunately, learning about it is a valuable investment with many dividends and benefits for our home, family, and office. Security and privacy are improved, and so is efficiency. Once we have improved our skills, we are better prepared to help our clients—individuals and small businesses that face similar threats and risks.

Doing nothing is unacceptable, so let's resolve to start eating the proverbial elephant one bite at a time. This may be an unfortunate analogy and mental image—especially in a time of elephant poaching and habitat destruction—but you get the idea.

THREATS AND RISKS

Until we understand the evolving threats, it is hard to use our common sense for risk analysis and defense. Cybercrime for profit is a global economy that targets everyone, regardless of occupation, position, or wealth. Anyone with a computer, e-mail account, Internet connection, financial account, or the ability to obtain credit faces threats. This means everyone is at risk. Cybercrime and identity theft are criminal capitalist marketplaces with participants of many skill levels, attempting scams of different types, trying and innovating until they find schemes, partners, and victims that earn them money. General schemes involve (1) infecting computers; (2) taking over electronic accounts, including e-mail accounts and financial accounts; (3) stealing data and using it for fraud; and (4) tricking victims into doing something (social engineering).

We all need to think about providing reasonable security for our systems and data, just like a landlord needs to provide reasonable security for tenants—which starts with a working lock on the front door. Attorneys face elevated threats and potential harms because they and their clients have been specifically targeted and victimized. Attorneys have duties of competence and confidentiality that mandate appropriate cybersecurity. Much ink (and many electrons and photons) have been spilled toward explaining these duties, which seemingly can be summarized as "it depends" and do what is "reasonable." "Reasonable" may seem vague, but we know what is unreasonable—doing nothing and ignoring

By John Bandler

basic security principles. If you never get started, this means a failure to assess your circumstances and what measures are appropriate. So get started, think about the threats and principles, evaluate the risks, make decisions, and take some actions. Attorneys also play an important role in the transfer of funds and assets on behalf of clients, and this requires special attention to the associated cybercrime and fraud risks.

Information security can be summed up with the initialism "CIA": Confidentiality, Integrity, and Availability.

INFORMATION SECURITY PRINCIPLES

The most important information security principle is easy to remember with the initialism CIA: Confidentiality, Integrity, and Availability. *Confidentiality* means keeping your information and data from being stolen or viewed by people who are not supposed to view it, including keeping hackers out of your computer and e-mail account. *Integrity* means keeping your data from being tampered with, which could include ensuring that a hacker doesn't send e-mails from your e-mail account or ensuring that your website or social media page isn't hacked or defaced with inappropriate messages. A more traditional example of data integrity is when financial firms ensure that no one can tamper with their records, including account balances and transactions. *Availability* means being able to access your data and systems. Ransomware is an attack on availability by encrypting and locking up the victim's data. We want our systems and data to remain accessible to us, so a crashed hard drive or forgotten password can also affect availability.

Confidentiality and availability are often at odds. You can increase your security level and increase the confidentiality of your systems, but sometimes that means you have a harder time accessing them. Suppose you decided to do away with your home's front door—it will be easier for you to enter and exit, but you will have eliminated security and privacy and you'll be unable to keep the weather out. Add a door, and now you have to open and close the door each time you enter and exit, but we are all accustomed to that. Add a lock, and you can decide when to lock the door and when not to. Now imagine adding a second and third deadbolt to the door, each requiring a separate key, and also an alarm system with a keypad near the door to activate and deactivate it. You've decreased the ease of entering and exiting your home, but perhaps you have increased security significantly. Similar trade-offs apply with our electronic systems, but without sufficient technical awareness, some people are leaving their electronic doors wide open.

The information security principle of "least privilege" is similar to the concept of "need to know," meaning that people, devices, and software should have the capabilities and data they need, but no more. Consider a guest in your home or office who needs to connect to the Internet—you provide this Internet access, but the guest should not also get access to your network and data. If your child needs to use your computer to write a paper, the child does not need access to your sensitive or client files, nor the ability to install programs onto the computer.

The National Institute of Standards and Technology (NIST) cybersecurity framework sets forth the concepts of identify, protect, detect, respond, and recover. Consider also another framework called the Critical Security Controls (initially developed by the SANS Institute, now administered by the Center for Internet Security), which provide for 20 areas of increasing priority, starting with an inventory of computing devices—an easy step for all of us to perform—and ending with penetration testing, or "ethical hacking."

I have consolidated these 20 critical controls into three main areas that are helpful for individuals, small firms, and businesses to use in order to conceptualize and implement their cybersecurity: *devices, data,* and *networks.* Devices are what we put our hands on every day, and they need to be the first priority for security. Until we have secured our devices, we cannot secure our data, and if we don't understand our devices, we can't hope to understand our data and networks. Next we evaluate our data, where it is, and how it is secured and backed up. Finally, we evaluate our networks and Internet connections and how they are secured.

Throughout the process, the focus is not just security but efficiency and availability, as well as gaining knowledge and technical skills at an individualized pace. Cybersecurity and anti-fraud should be a part of your business planning and IT implementation, not something you try to bolt on later. I also recommend the concept of a cybersecurity risk dial. Consider where your security dial is set now and where you want it to be in the future, and move the dial thoughtfully and slowly. Don't react based on impulse and fear but make thoughtful and incremental changes you can live with.

DEVICES

Periodically—and now is a good time—make a mental inventory of your devices and review their settings. Physical control of your devices is the first priority, so develop good habits to prevent loss or theft. All of us can become distracted or forgetful, and opportunistic street thieves abound, so keep mobile devices on your person whenever possible, in a pocket or in a purse that always stays with you. Review device settings to ensure they require

a password (or fingerprint) to unlock and that they auto-lock after a period of inactivity. Review the software installed on the device, and review the device's privacy and security settings. Software should be from reliable vendors, running only when you need it, and should have access only to the data that it needs. Don't expect to learn everything about every program, but periodically review your privacy and security settings and installed programs because each time you will learn something new. Keep the operating system and software in your devices updated (patched), and run a malware scan on all the data in your laptops and desktops using an anti-malware product from a reliable vendor. There are many excellent, free anti-malware products to choose from.

DATA

You store data on each device—including hidden data you might not be aware of—and each device accesses data stored in the cloud. Periodically review your data, where it is stored, how it is secured, and when it was backed up. Your attic and closets get cluttered, and so do the places you store data. Organize your data periodically, and securely delete unneeded sensitive data. Sensitive data that leaves the home or office within a phone, tablet, laptop, or external hard drive should be encrypted; evaluate which of your devices are secured by full disk encryption. When you stop using an older device, ensure data—including residual data—is securely deleted before you sell, donate, or recycle it.

We all store enormous amounts of data in the cloud—including our e-mail accounts—which need to be secured properly. Secure cloud accounts with strong passwords and two-factor authentication (also called two-step log-in). If your e-mail account is secured only by a password, then it is vulnerable to being hacked because passwords are frequently stolen and can also be guessed. Criminals all over the world hack into e-mail accounts, review the contents, and also send e-mails as if they are the account holder. Enabling two-step log-in helps prevent this: Even if the criminal obtains your password, he still needs the one-time code sent to your smartphone, and without this code the criminal cannot access the account. Enable two-factor authentication for all your important Internet accounts, and periodically review all their security and privacy settings.

BUSINESS E-MAIL COMPROMISE AND CEO FRAUD

Business e-mail compromise and CEO fraud are rampant frauds that have stolen billions of dollars, relying on trickery to get victims to authorize wire transfers to accounts controlled by the criminals. Often these scams involve a hacked e-mail account that criminals monitor for days, weeks, and even months waiting for an opportunity. Then, the hacker directs funds be wired to an account controlled by an accomplice and works to delay discovery of the theft, making the funds nearly impossible to recover. There are variations of these frauds, some of which do not require the e-mail account to be hacked.

The first defense against this fraud is to protect your e-mail account from being hacked, as we discussed previously. The next defense is to ensure that any financial payment instructions are confirmed through a verbal conversation—an essential anti-fraud measure that also helps our mental health and client relations. To reiterate, any payment instructions relayed from one person to another needs to be followed by a verbal confirmation, even where there are many people in the communication chain, such as seller, seller's attorney, buyer's attorney, and buyer. Clients should be advised in advance about this fraud risk and should be informed that they must verbally confirm any payment instructions—and any changes to the instructions—that they receive. Red flags include a need for immediacy and an inability to speak by phone.

NETWORKS AND THE INTERNET

Imagine if everyone's front door locks could be opened with the same key. Many people's networks are configured like this because routers are often sold with a default username and password such as "Admin/Admin," and many people never change them. Your router has a number of other settings that affect security, and these should be reviewed periodically as well.

All networks—but notably public WiFi networks—are shared environments that we should think of as a crowded event where someone might eavesdrop on your conversation or even pick your pocket. Avoid or limit your use of public WiFi, and use encrypted communication whenever possible through the Internet. For example, an HTTPS website encrypts its communication with you, whereas an HTTP website does not. Most e-mail providers now encrypt their communications with you, and this provides considerable protection on these shared networks.

CONCLUSION

We covered a lot of ground in this short article, and the main lesson should be that cybersecurity, privacy, and anti-fraud are for everyone, including you. There are plenty of good resources out there to help you learn more, and I would immodestly suggest that my book (*Cybersecurity for the Home and Office: The Lawyer's Guide to Taking Charge of Your Own Information Security,* ABA, 2017) is one of them. Don't be intimidated, but also have a healthy respect for some of the complexities involved so that you do not start an enormous task before your skills are ready for it. Resolve to increase your knowledge and skills continually, knowing you will be able to employ them for your home, family, office, and clients. ■

John Bandler (johnbandler@bandlergroup.com) is founder of Bandler Law Firm PLLC, which helps firms, businesses, and individuals with cybersecurity, cybercrime investigations, litigation support, and other areas. Previously, he was a state trooper, then a prosecutor who investigated global cybercrime. Now he is the author of the book *Cybersecurity for the Home and Office: The Lawyer's Guide to Taking Charge of Your Own Information Security* (ABA, 2017). For more information, please visit cybersecurityhomeandoffice.com.