Make Cybersecurity a Priority

In her Best Practices for Solo Practices column, Janet Falk offers up some seasoned tips and advice from solo attorneys on how they exercise best practices in cybersecurity.

By **Janet Falk** October 28, 2019 at 12:30 PM

Janet Falk

October is *National Cybersecurity Awareness Month*, making it timely to consider how solo attorneys exercise best practices in cybersecurity.

Forty-three percent of online security incidents target small businesses according to the Verizon Data Breach Investigation Report (2019). Such attacks may lead to financial loss, theft of customer data or proprietary information being compromised.

As a solo attorney, who may advise clients in the small business category, the threat of a cybersecurity attack or breach is an important concern not only for your own practice but for your clients as well. According to computer security expert Bruce Schneier, “You can’t defend. You can’t prevent. The only thing you can do is detect and respond.”

Attorney Abraham Perlstein of **The Law Office of Abraham J. Perlstein**, who practices in the cybersecurity area, agrees with Schneier. “As an attorney, you should take pre-emptive steps and take actions to set yourself up to defend and protect yourself, and your clients, to the extent possible and to be able to show that you have done so.”

Passwords

To begin your cybersecurity audit, consider your use of *passwords* to open your computer, access cloud-based storage and utilize legal research databases, among other websites. Barry Heyman, with a practice in entertainment, music, new media and IP at **Heyman Law**, says “I use unique, strong passwords, change them periodically,

and I use two-factor authentication." According to Heyman, "Two-factor authentication is one of the most important security measures, because it is much less likely that you will be hacked and you receive notice if there is a suspicious login attempt." The nightmarish experience of a friend whose password was stolen demonstrates "the extra time it takes to secure your accounts is definitely worthwhile."

For those who record their passwords in an Excel spreadsheet or document on their computer, be aware that a hacker will review ALL your files, so that is not a 100%-secure solution. Consider printing the list, filing the document safely and using it like a map to re-orient yourself. Additionally, Perlstein counsels against storing passwords on a given website when you login to that site. Instead, type in the password each time you visit a website that requires a password, especially websites for your financial accounts.

Many solo attorneys find password managers, such as LastPass, helpful in remembering and storing their many passwords.

Backing Up

Backing up documents and files is the best cyber-insurance. Patricia Werschulz, who practices patent and trademark law at **Werschulz Patent Law** uses Time Machine, a built-in feature on the Mac computer. It "automatically backs up on external hard drives. I have one at home and one in the office, so each day my hard drive is backed up in two geographically different places." Perlstein applauds backing up files daily as an ideal; if not, back-ups should be performed at least weekly, perhaps at the close of business on Friday.

Zara Watkins, with a practice writing briefs for appeals and substantive motions in state, federal and immigration cases at **On Point Expertise**, notes "All of my documents are uploaded to a cloud-based system immediately," which serves as an electronic back-up.

Another approach regarding back-ups, and with the feature of file-sharing, is Dropbox.com, where files are instantly and automatically backed up. In addition, users

may share a link that will grant access to folders and files and designate whether the recipient may view and/or edit the document. Andrew Berks recommends Dropbox and has also used Hightail to exchange large files with others in his intellectual property, patents and litigation practice at **Berks IP Law**. An additional precaution is to use Dropbox in conjunction with a cloud-based back-up service, as recommended by Sean O'Rourke, Cyber Liability Consultant at **Combs & Company**.

Update

It's important to update the software systems and programs you use, whenever new versions come to market. Eric Sarver, who represents businesses in employment law matters at **The Law Offices of Eric M. Sarver**, notes "I update my security software frequently, both when prompted to by my computer/software and when my cybersecurity consultants let me know" to do so. Heyman is a bit more wary, saying "I update as soon as practicable, but I first search the Internet for reports of bugs in the updates and I wait until the update is known to be safe and secure."

Keeping Up

Cybersecurity issues can be overwhelming to an attorney with a solo practice. Werschulz takes CLEs to keep up-to-date on these issues, as does Watkins, who "regularly watches webinars, because it's important and fast-changing." Berks reads computer industry newsfeeds to train himself. He also asks the colleagues he works with to use two-factor authentication and encourages them to use appropriate password practices.

Protecting Clients

As for reminding clients of their own cybersecurity awareness, Heyman notes "I promote cybersecurity awareness through occasional newsletters and social media posts." Sarver says, "I advise my clients to be mindful of suspect files, emails with attachments from unknown senders, and other items that might be corrupted."

For Watkins, the issue in dealing with her clients is not cybersecurity, per se, but redaction of personal information. These may be included in documents and records that have already been submitted to the court and which she reviews in her appellate practice. Watkins notes, “I tell my clients that if they think there is any chance there is sensitive information (like Social Security numbers) in the documents to advise me ahead of time, so I can secure my receipt of the documents, redact them myself, and then delete traces of it from my email program. That way, I never have sensitive information on my email or cloud-based storage system.”

Outside Help

External services may also provide support in cybersecurity matters. Eric Sarver has contracted with an outside consultant, Threat Condition, “to strengthen the protections I had in place.”

Andrew Berks notes that the third-party billing services, such as Quickbooks and Freshbooks, invest heavily in their own security systems. A colleague “had an incident where an invoice was apparently altered in transit to change the payment instructions, and the client payment went to a fraudulent account.” Relying on the secure distribution of such a vendor would have averted that outcome.

As you review your own cybersecurity practices, you may discover you are not following some of the back-up, cybersecurity training, software updates and password practices of your colleagues. Do not be discouraged. Instead, plan to make appropriate changes and improve the security of your files and your online accounts.

To end on a lighter note, consider the password practice of Charles-Eric Gordon, investigative counsel at **Law Office of Charles-Eric Gordon**, who has an unusual approach. Gordon uses “former addresses and phone numbers of not too-closely related family members and friends. Even if one needs a clue to remember the password, a reference to Uncle Max or Jennifer won’t be easily deciphered.”

October and Cybersecurity Awareness Month are about to end, yet best practices for cybersecurity clearly are a year-round concern. Start your cyber-review today.

Janet Falk *is the head of Falk Communications and Research in New York. She provides media relations and marketing communications services to law firms and consultants. She may be reached at (212) 677-5770 or Janet@JanetLFalk.com.*

https://www.law.com/newyorklawjournal/2019/10/28/make-cybersecurity-a-priority/