New Jersey Law Journal

Solos and Small Firms: Conduct Your Cybersecurity Check-up

October is National Cybersecurity Awareness Month, which makes it timely to consider the best practices solo attorneys follow to manage their cybersecurity.

By **Janet Falk** | October 06, 2020

Credit: ImageFlow / Shutterstock.com

Cybersecurity is an ongoing concern; October is National Cybersecurity Awareness Month, which makes it timely to consider the best practices solo attorneys follow to manage their cybersecurity.

William Denver, of **The Denver Law Firm** in Red Bank, with a practice in litigation and insurance recovery, makes cybersecurity issues a priority,

following his experience with an attack by a cyberhacker when he was a partner at an AmLaw 100 firm. The breach “disabled a number of the laptops with ransomware. Most of the documents were backed up on an internal server, but a few were not, and some projects had to be recreated.”

Learning from that incident, Denver has automated the backup process to avoid losing valuable documents and emails.

Backups are only one element in your approach to the cybersecurity issue. As a solo attorney, you must keep your own security issues top of mind, and also advise your clients to take similar measures. As Bruce Schneier, a computer security expert, said “You can’t defend. You can’t prevent. The only thing you can do is detect and respond.”

Conduct a quick check-up of *your* best practices for cybersecurity: back-up and cloud-based storage; passwords and cybersecurity training, plus advice to clients on texting and social media.

Solo attorneys are well-advised to use automatic backup systems that are based in the cloud. For Rajeh Saadeh, “Files are backed up automatically in the middle of every evening. Our files are found on a server, and the automatic backups are made to a different server in a different location. That way, in the event something catastrophic happens, like the building burns down or there is water damage or the server is stolen, all of our files are intact in a separate location.” Saadeh has a matrimonial and real estate law practice, **Law Office of Rajeh A. Saadeh**, in Somerville.

Ayesha Hamilton, with a practice in business and employment law at **Hamilton Law Firm** in West Windsor, takes a similar approach. “I use a cloud based backup which is set to back up every few minutes. You can also trigger

it to run a backup manually and this program will send you an email notification if a backup has not happened in a day or two."

Keeping documents in the cloud permits a solo attorney to view them at any time and in any location. According to Judie Saunders, "I found cloud computing to be essential for an agile boutique firm. Responding to clients is important and with cloud computing you have access to review information remotely and provide information clients need." Saunders' practice at **The Law Office of Judie Saunders**, offers legal counsel and litigation services to sexual, physical and psychological survivors, personal injury and criminal defense, with offices in Red Bank and New York City.

Saadeh agrees that instantaneous access is invaluable. "Our server is cloud-based so that everyone in the firm is using the same files no matter where they are, whether it be in the office or elsewhere, such as working remotely or even in court."

Hamilton says, "I use Google Drive for all case related documents now and Sharefile to share discovery and documents with adversaries, as well as clients."

Sean O'Rourke, Cyber Liability Consultant at **Combs & Company**, notes, "An additional measure when using services like Google Drive, Dropbox, or other file sync services is to augment it with a cloud-based back-up service. While the sync feature may appear like a backup, it is not."

When it comes to passwords, cybersecurity attorney Ryan Cooper stresses the importance of safeguarding them by using complex passwords comprised of letters, numbers and symbols *and* a password manager. Cooper says, "Use strong passwords and don't reuse them, no matter how complex. A password

manager has an institutional level of security to manage your password database."

In addition, Cooper adds, "Access to the firm's software or external accounts, for example Westlaw, usually requires a password. In that instance, your firm can have a single login that is accessed via the password manager without the actual account password being visible." Cooper's practice in privacy, cybersecurity, insurance recovery and litigation, **Cooper LLC**, is located in Cranford.

Hamilton remarks "I make sure that I do not allow my computer to save passwords for certain sites like banking, email, Google drive, Sharefile, etc."

How do solo attorneys keep up to date with cybersecurity training? Some vendors conduct webinars for their attorney customers, often for CLE. Saunders says "Our firm takes advantage of the bar's CLE access pass for small firms, which allows enrollment in cybersecurity and other trainings, so we can remain current and best service clients." Cooper recommends attorneys attend at least one hour of training annually to keep up with the fast-moving sector.

As Chair of the Solo and Small-Firm Committee of the New Jersey State Bar Association (NJSBA), Denver points out the association provides training and resources. "The NJSBA takes cybersecurity of its members very seriously. Last year, at the Solo and Small Firm Section, there were two cybersecurity panels which included the head of IT security for the New Jersey Courts. We also discussed the importance of cyber insurance products, how many of them have different coverage terms and that it is crucial for firms to tailor their cyber insurance policies to cover their unique business and client risks.

Members can access written materials from these and other cybersecurity panels in the member CLE portion of the NJSBA website."

As for recommendations and interactions with clients on issues of cybersecurity, Hamilton advises clients that text messages are not secure. For Saunders, the documentary film *Social Dilemma* "made me aware of another level of security that firms and attorneys must consider, namely ensuring the security of the firm's and client social media activity. The nature of my practice requires that clients be made aware that they should use an extra layer of security and be aware of their online activities."

Finally, O'Rourke and Denver note that attorneys and staff should be trained to spot *phishing* emails, namely, attempts to lure an unwitting email recipient to click on a link that may lead to malware being downloaded onto a computer. Denver's team is on the alert for "anything that looks even remotely suspicious; we do not open it. Recently, we were negotiating a settlement agreement with one of our adversaries and we received a purported *draft settlement agreement* with a link my adversary had not utilized in the past. We called the adversary and learned his email had been hacked."

Cooper advises that cyberhackers are looking for low-hanging fruit. By employing reasonable cybersecurity precautions—installing software updates, using strong passwords with two-factor authentication, encrypting email and files—you will deter most hackers from attempting to break into your systems.

Actively monitoring cybersecurity is vital to the health of your practice, during October's Cybersecurity Awareness Month and throughout the year, especially now that the courts are conducting considerable activity online. Plan to adopt these best practices regarding backup, passwords, training and

counsel to clients to ensure the safety of all your documents, records and accounts.

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/njlawjournal/2020/10/06/conduct-your-cybersecurity-check-up/