

YOUR COMPUTING SECURITY CHECKLIST

Ellen Freedman, CLM
Law Practice Management Coordinator
Pennsylvania Bar Association

Each of you have attended at least one, and most likely several, cybersecurity seminars by now, hosted by various presenters, alerting you to the various computing risks we face daily.

Most seminars have included more than a few words about your ethical responsibilities to take reasonable steps to safeguard the confidentiality of your clients and your client's property.

If you attended one of my seminars, you know that every day, new risks arise. New viruses are created and released into the wild. New criminal syndications arise to create additional ingenious schemes to trick or entice you and your staff into clicking on link, entering confidential passwords, or wiring out money. New ransomware is unleashed.

In short, we are constantly aiming at a moving target. So, what you learn and do today to protect your firm and its clients, may not be sufficient tomorrow.

In looking back at the many articles I have written on the topic over the years, I realize that while each may contain specific advice, nowhere have I consolidated everything into a simple checklist. It's overdue.

I want to ensure that computing security is incorporated into your routine business practice. Every year you complete and submit an updated application for professional liability insurance. Going through that process often causes you to make important changes.

For example, a new question is asked, such as whether you have a surrogacy agreement, and it causes you to pause and realize you should be answering "yes" if you are a solo attorney. In the same manner, every year you should be going through the computing security checklist to ensure you are continuing to take

reasonable precautions based on current threat levels and your computing environment.

Annually

Each year you should do the following:

- ☐ Have a cybersecurity audit performed in the final quarter of the year. Be sure to include systems of remote workers, if recommended by the auditor. (This will be based on the sophistication and type of connection you provide for each.)
- ☐ Based on the audit recommendations, get pricing for any necessary upgrades or fixes. Adjust your IT budget for the following year accordingly.
- ☐ Review your computer use policy and procedures for any necessary updates. Be sure to communicate any changes to everyone at the firm.
- ☐ Check security policy and practices from critical key computing vendors to ensure they continue to meet standards.
- ☐ Check security on any equipment which provides connection directly to the internet, which may include multifunction devices, printers and so forth. (This may be included in cybersecurity audit.)
- ☐ Check for any information of the firm on the dark web and make internal changes to logons and passwords appropriately. (This is usually an optional service from the firm's cybersecurity company or auditor.)

Ongoing

- ☐ Appoint someone at the firm responsible for being risk-aware and ensuring compliance with firm policies and procedures. This person should regularly monitor and be aware of new emerging threats and make sure the firm's security set-up adequately provides continued protection. If no one is available at the firm, the firm should consider out-sourcing this function.
- ☐ Ongoing training for all at the firm, including owners, in phishing attempts, business email compromise and current threats. Provide at least quarterly reminders of breaches occurring at other firms and how they happened.
- ☐ No one-time money transfers outside the firm without confirming email instructions with a phone call.
- ☐ No last-minute changes to money transfers without confirming email instructions with a phone call.

- Use good password managers. All passwords should be complex and stored in encrypted format in a password manager that is accessible by at least one owner of the firm. Memory issues are eliminated when password managers are used.
- Require quarterly or semi-annual password changes for all accounts which provide access to money or credit cards / purchasing.
- Use a virtual private network (VPN) on all mobile devices when on public or unowned Wi-Fi.
- Backup the computers to two locations daily. One system should be in the Cloud.
- Use anti-malware and antivirus software that automatically updates at least once a day. Be sure it is configured properly to exclude large databases like time & billing software. It should be set to scan automatically throughout the day or night.
- Use anti-virus web browsing security to block connection to infected or malicious websites.
- Enable two-factor authentication on every website and service where it is available.
- Monitor the status of all software used by the firm. Discontinue use of ***any*** software that is out of support. Using these are like leaving the bank vault door unlocked. A breach that results will certainly expose the firm to ethical sanctions for unsafe and unreasonable practices.
- All communications with clients should be secure and preserved as part of the file. Examine non-traditional methods, such as text messaging, to ensure compliance. Implement a secure platform if necessary. Note that client portals in practice management (case management) software are excellent solutions.
- Reevaluate the firm's method(s) for storing and exchanging documents to ensure security, confidentiality, and preservation.
- Ensure that the firm's website is still adequately protected by anti-malware, unauthorized insertion(s) of code or other changes and properly backed up.
- As inter-connectivity between applications and Cloud service providers increases, perform security due diligence to ensure no new exposures are created.

I welcome anyone to help me add to this checklist. I'm sure I haven't thought of all the best practices to include and perform regularly. But I can assure you that if you follow this checklist, you and the firm will be taking sufficient reasonable precautions to meet your ethical requirements.

Let me be clear. Following this checklist doesn't ***guarantee*** that your firm will not suffer a security breach. No one can guarantee that. But the odds will be in your favor to avoid it. Hackers aim for easy targets. With sufficient roadblocks, your chances are good they will move on. However, if they are determined, they have unlimited tools at their disposal, including the sheer horsepower of botnets of thousands of computers which can be aimed at your back door.

Remember also, it only takes one person a careless moment to click on a malicious link. Then, no matter how high your security spending, or how great your methods and policies, it won't matter a bit. You're only as strong and protected as your weakest link in the chain.

Share your reactions or comments to this article with Ellen Freedman at ellen@freedmanlpm.com.

A version of this article originally appeared in the October 24, 2022 issue of the Pennsylvania Bar News.

© 2022 Freedman Consulting, Inc. The contents of this article are protected by U.S. copyright. Visitors may print and download one copy of this article solely for personal and noncommercial use, provided that all hard copies contain all copyright and other applicable notices contained in the article. You may not modify, distribute, copy, broadcast, transmit, publish, transfer, or otherwise use any article or material obtained from this site in any other manner except with written permission of the author. The article is for informational use only and does not constitute legal advice or endorsement of any particular product or vendor.