

Cybersecurity Checklist for Solo and Small Firm Lawyers

Disclaimer: This material is intended as only an example which you may use in developing your own form. It is not considered legal advice and as always, you will need to do your own research to make your own conclusions regarding the laws and ethical opinions of your jurisdiction. In no event will ALPS be liable for any direct, indirect, or consequential damages resulting from the use of this material.



Meet Mark:

Mark Bassingthwaighte, Esq., serves as Risk Manager at [ALPS](#), a leading provider of insurance and risk management solutions for law firms. Since joining ALPS in 1998, Mark has worked with more than 1200 law firms nationwide, helping attorneys identify vulnerabilities, strengthen firm operations, and reduce professional liability risks.

He has presented over 700 continuing legal education (CLE) seminars across the United States and written extensively on the topics of risk management, legal ethics, and cyber security.

A trusted voice in the legal community, Mark is a member of the State Bar of Montana and the American Bar Association and holds a J.D. from Drake University Law School. His mission is to help attorneys build safer, more resilient practices in a rapidly evolving legal environment.



Contact Information:

Mark Bassingthwaighte, Esq.
ALPS Insurance Agency
111 N. Higgins Ave, Suite 600
Missoula, MT 59802

(T) 800.367.2577 | (D) 406.523.3859

mbass@alpsinsurance.com

www.alpsinsurance.com



This checklist is intended to help those who have a desire to become more cyber-secure know where to start. It may also be helpful in identifying areas of concern that can, and should, be discussed with IT support personnel. Most importantly, be aware that cybercrime attack vectors will continue to change and evolve as will the sophistication of the attacks. Becoming cyber secure is an ongoing process, not a one and done effort.

Minimum Security Baseline (Core Protections)

- Institute a password policy that mandates the use of strong, unique passwords for every application and account that will accept them and store them in a password manager. Strong passwords are defined as, being 22 characters or more in length using a combination of uppercase and lowercase letters, numbers, and special characters. Note: Every account and application in use should have its own unique password, and no password should ever be reused once changed.
- Require a password, PIN, or biometric lock on every device used for work.
- Enable multi-factor authentication (MFA) wherever possible to make it much harder for attackers to gain access even if a password is stolen. This is particularly important with email, cloud services, banking and financial sites, and practice management systems.
- Keep computers, phones, and tablets updated with the latest security patches and operating system updates; and keep all software applications on all devices up to date by promptly installing all security patches as they are released.
- Install and maintain reputable antivirus or endpoint security software on all devices used for work.
- Mandate that all work-related Internet sessions be encrypted and prohibit the use of unsecured open public Wi-Fi networks. This does mean that remote access to the office network must always occur using a VPN, MiFi, phone tethering, or some other type of encrypted connection.



- ❑ Ensure that every firm and home office Wi-Fi router is password protected, uses modern encryption (WPA2 or WPA3), and has the default administrator password changed.
- ❑ Enable automatic screen locking on all computers and mobile devices.
- ❑ Enable remote wipe capability for all smartphones and laptops in case of loss or theft.
- ❑ Maintain regular backups of all critical data, periodically do a test restore of a backup, and store the backups in accordance with a disaster recovery plan because floods, fires and ransomware attacks happen. Backups should also be encrypted when taken off site or stored in the cloud. If using a cloud vendor, the vendor should not have access to the decryption key.
- ❑ Only use secure cloud services that provide encryption and strong authentication protection.
- ❑ Ensure all lawyers and staff receive basic social engineering awareness training monthly at minimum.
- ❑ Properly dispose of any device or digital media that has or had any business-related data on it. Don't overlook personal devices used for work, digital copiers, digital cameras, memory cards, CDs, DVDs, jump drives, backup tapes, etc. All devices and media must be digitally wiped clean and/or physically destroyed. This does mean that devices cannot be given away for personal use, donated, recycled, or sold unless the entire drives have been overwritten. Side note: a restore to factory default settings is not an acceptable alternative to wiping a drive.

Enhanced Cybersecurity Protections (Stronger Security for Higher Risk Profiles)

Devices and Access

- ❑ Enable full-disk encryption on all laptops and mobile devices.



- ❑ Mandate that everyone turns off Bluetooth and file-sharing features when not in use.

- ❑ Maintain an inventory of all devices used to access firm data and determine where all office data is stored by creating a network diagram. Make sure this diagram remains current because it will be useful to digital forensic experts in the event of a security breach. In addition, this diagram can and should be used to create a security policy that responsibly addresses every situation where any data resides.

- ❑ Prohibit the jailbreaking of any mobile device that will be used for work because jailbreaking makes the device far more susceptible to a cyberattack. Jailbreaking is defined as modifying the operating system from its original state.

- ❑ Restrict access to firm systems so that only authorized users can log in.

- ❑ Use separate user accounts for each individual rather than shared logins.

- ❑ Limit or avoid using personal devices for firm work or ensure they meet firm security standards.

- ❑ Never allow a non-employee to have access to your network absent appropriate oversight. In a similar vein, immediately cut off all avenues of access to the network for anyone who has been terminated. Terminated individuals should never have access to any office computer or network plug absent a trusted escort, even if their stated intent is to only download personal files.

- ❑ Remove unused and unnecessary software and applications from all devices.

Network Security (Office and Home)

- ❑ Keep router firmware updated and periodically review router security settings.

- ❑ In order to prevent unauthorized access to your firm's confidential data, create a separate Wi-Fi network for guests and the use of personal devices.



- ❑ **Disable automatic connections to unknown wireless networks on all devices.**
- ❑ **Mandate the use of a Virtual Private Network (VPN) when anyone is working remotely or traveling.**
- ❑ **Keep your server in a locked room because physical security matters!**
- ❑ **Check your internal and Internet-facing network security at least annually to make sure your network is secure. This can be done by having a vulnerability assessment or penetration test done.**

Cloud Storage and Online Services

- ❑ **Confirm cloud providers encrypt data in transit and at rest. If they don't, you should encrypt your data before placing it in the cloud. Just make certain you properly secure your encryption key, so you never lose it – think password manager.**
- ❑ **Review data access permissions to ensure only authorized users can view client files and remember to remove access when someone no longer needs it or departs the firm.**
- ❑ **Enable activity alerts or login notifications for important accounts.**
- ❑ **Conduct periodic reviews of all third-party applications connected to your cloud accounts to ensure that only essential applications remain in use.**

Email and Communications Security

- ❑ **Use spam and phishing filtering tools for email.**
- ❑ **Avoid sending sensitive information through unencrypted email when secure alternatives are available, such as the use of a client portal.**



Use of Artificial Intelligence and Generative AI Tools

- ❑ Avoid entering confidential or privileged client information into public generative AI tools unless the tool is approved and secure.
- ❑ Understand how AI tools store, process, or train on submitted data before using them.
- ❑ Review AI-generated output carefully for accuracy and reliability.
- ❑ Establish firm guidelines for when and how AI tools may be used in legal work.
- ❑ Confirm whether AI vendors retain or reuse prompts and uploaded data.

Vendor & Third-Party Management

- ❑ Avoid free or consumer-grade tools for storing or transmitting client data.
- ❑ Vet third-party vendors (cloud storage, billing software, virtual assistants) for cybersecurity compliance.
- ❑ Ensure vendors sign confidentiality or data protection agreements.
- ❑ Limit third-party access to client data when possible.

Public Computers and Shared Devices

- ❑ If at all possible, never access client files or firm systems from public computers.
- ❑ If public access is unavoidable, use a private browsing window, avoid saving credentials, and log out of all accounts afterward.
- ❑ Do not download or store client documents on shared or public computers.



Incident Response and Recovery

- **Develop a basic incident response plan outlining what to do if systems are compromised.**
- **Know who to contact for IT support and cybersecurity assistance in an emergency.**
- **Establish procedures for notifying clients or authorities if a breach occurs.**
- **Periodically test backup restoration and recovery procedures.**