CHECKLIST TO PREVENT AND PREPARE FOR A DATA BREACH

Lawyers are entrusted with vast amounts of client information. If not protected, this information can be exposed or disclosed to unauthorized parties. Cyberattacks, lost or stolen devices, or other security incidents can result in a data breach that may have devastating consequences for a law firm and its clients. This checklist is intended to provide guidance on how to prevent and prepare for a data breach.

Enlist IT Support

1. If you don't have in-house IT, find a third-party IT professional who can provide technical support for your firm.
2. This person can help you assess your security situation, determine the necessary steps to prevent and prepare for a data breach, and be available when you have questions or need assistance.

Perform Risk Assessment

3. Conduct a risk assessment to identify all the threats to and vulnerabilities of your firm's system. Your assessment should address the following:
    a. What data does your firm hold? (e.g., client names and contact information, Social Security numbers, financial information, medical records)
    b. Where is the data being stored? (e.g., onsite file cabinets, onsite server, unencrypted desktop computers, cloud storage)
    c. Who has access to the data? (e.g., attorneys, staff, third-party vendors)
    d. What are the weaknesses in your system? (e.g., lax or no building security, older computer, expired or no virus protection software, weak passwords, insufficient staff training, irregular or no backups)
4. List the issues identified during the assessment.
5. Work with your IT person to fix the vulnerabilities in your systems.

Risk Areas to Assess and Shore Up

6. *Secure Your Remote Work Environment.* Working remotely can be a security risk because staff may have unsecured devices or weaker security setup and controls at home than at the office. This makes remote staff more vulnerable to cyberattacks.
    a. Devices – Require staff to use firm-owned and controlled devices rather than home machines for their work.
    b. Remote desktop protocol – Use Remote Desktop Protocol (RDP) together with a virtual private network (VPN) to access your work computer from your remote office. See this article for more information: https://www.osbplf.org/blog/inpractice/remote-access-for-lawyers--remote-desktop-protocol-rdp-and-virtual-private-network-vpn/.
    c. Secure wireless – Ensure that your wireless network is secure when working remotely. Do not share your internet with neighbors. Provide house guests with separate Wi-Fi guest access to limit exposure of your network. Get sufficient bandwidth so internet connections do not get dropped or disconnected.
7. *Secure Your Internet Connection and Practice Safe Internet Usage.* All electronic communication is routed through your wireless network. An unsecured wireless network is vulnerable to unauthorized access by hackers, and the data transferred on the network will be exposed.
    a. Wi-Fi protected access (WPA) – Ensure that your wireless network is protected by encryption using WPA2 or WPA3. Your internet service provider can set this up. Ask

them to show you how to change the password and access your wireless network connection on your computer.

b. Public Wi-Fi – Don't use public wireless without using a virtual private network (VPN) or a smartphone hotspot.
c. Safe browsing – Make sure you have current spyware and phishing protection enabled. Follow a safe internet browsing protocol by using a website filter, accessing only secure websites with "https" in the address, heeding security warning messages, and not clicking on random pop-up ads or suspicious links. Also avoid downloading anything from the internet that might contain malware.
d. Firm devices – Do not download and install programs or applications on devices used for work without prior authorization from management and IT. Don't use the internet on firm devices for personal use.

8. *Protect Your Computer Network.* Whether or not your firm has a computer network, it is crucial to protect both the network and the individual computers connected to it from various threats.
    a. Firewalls – Use a firewall to prevent threats from entering your devices. Many devices and routers have built-in firewalls, but they must be turned on, configured, and updated regularly.
    b. Antivirus software – Install antivirus software on all your devices. It will protect your device by detecting threats and removing them. Keep the software updated and run scans regularly.
    c. Endpoint detection and response – Install endpoint detection and response software monitors on all your devices to detect and alert you to threats that firewalls and antivirus software may have missed. Ensure the software has on-demand scanning and quarantine capabilities.
9. *Update Your Operating Systems and Software Programs Regularly.* Devices running on outdated operating systems and software programs that are no longer supported are vulnerable to malware and hackers.
    a. Regular updates – Install all operating systems updates, including updates to the programs and applications on your computer. Do not ignore your computer prompts to run updates. Regularly check for updates by going to your computer settings and installing them if available.
    b. Upgrade – Upgrade any device or application that is no longer supported by the manufacturer.
10. *Secure Your Data Storage.* Where you store client data can be an issue if the location—whether physical or online—is not secured. Ensure the location of data storage is secure against unauthorized access. Only grant access to authorized personnel.
    a. Physical storage – Contact your building manager or owner about installing security cameras on the premises and implementing other security features to limit access.
    b. Firm devices – Do not leave your laptop, phone, or any device containing client information unattended. Do not share your device with anyone else, including family members. Configure devices to lock with no ability to log on for a period of time after a certain number of failed logon attempts. Encrypt all devices, files, and folders. For more information about encryption, please see: https://assets.osbplf.org/in_briefs_issues/Protect%20Your%20Data%20by%20Using%20Encryption.pdf.

   c. Cloud storage – Use services that encrypt your data while in transit and at rest. For more information, please see: https://www.osbplf.org/blog/inpractice/understanding-security-when-using-cloud-storage/.

11. *Perform Regular Backups.* Avoid complete data loss by backing up your files and data. For more information about backups, see *How to Back Up Your Computer*, available on the PLF website, www.osbplf.org. Click on Services > CLEs & Resources > Practice Aids > Using Technology. Also see this article for more information: https://www.osbplf.org/assets/in_briefs_issues/Whats%20Backing%20Up%20Your%20Data.pdf
    a. Follow the 3-2-1 rule for backups – Have at least three copies of your data, including one original and two backups. Keep the data backed up on two different storage types. Keep at least one copy of the data offsite.
    b. Automatic and continuous – Backups should be automatic and continuous and should happen multiple times throughout the day using appropriate backup software.
    c. Secure and segmented – Have your IT person set up your backup system so it is secure and segmented or isolated from your original storage system to protect the backups so they cannot also be vulnerable to a cyberattack.
    d. Regular tests – Test the recovery from your backups regularly to be sure they are working properly.
12. *Securely Communicate Electronically.* Emails pose many risks because they are not encrypted by default and are a vector for phishing and spamming.
    a. Phishing – Don't open attachments in emails from strangers or even unexpected attachments from those you know. Contact the person by phone, using a number verified through a source separate from the email, to ensure they sent you the attachment. Don't click on links in emails, as they may contain malware or redirect you to a website that asks for your personal information.
    b. Spam – Install a spam filter on your email program to help identify emails that marketers or attackers send that may contain malicious content.
    c. Encryption – Consider using an email encryption program when sending confidential or sensitive emails. You can use encrypted webmail services like ProtonMail, Hushmail, or StartMail, or a third-party email encryption software like Trustifi, ShareFile, or Virtru. For a short-term measure, putting a password on a document helps encrypt the contents. See this article for more information: https://www.osbplf.org/blog/inpractice/easy-diy-encryption-for-emailing-documents/.
    d. Client portal – Securely exchange documents and messages with clients using secure client portals. Many practice management programs like MyCase, Clio, and Smokeball have built-in client portals ready for use out of the box. See this article for more information: https://www.osbplf.org/blog/inpractice/client-portals--take-control-of-client-communication/.
13. *Securely Exchange Information*. Unsecure file sharing may expose sensitive or confidential information contained in documents and other types of electronic files.
    a. Standalone device – When opening electronic files from outside sources, consider using a standalone device that is not connected to any firm network. Run your virus program to scan for any malicious software that may be embedded in the file.
    b. Secure file sharing – Do not mail flash drives because they are easily lost or stolen in transit. Consider using a secure file sharing program like ShareFile, Tresorit, TitanFile, or Lexshare.

c. Remove metadata – Always examine any data you are releasing to determine whether it contains sensitive or confidential information so you can take proper steps to protect it, including removal of metadata. For more information about proper removal of metadata, see the PLF practice aid *Removing Metadata,* available on the PLF website, www.osbplf.org. Click on Services > CLEs & Resources > Practice Aids > Cybersecurity & Data Breach. Also see this video at https://www.osbplf.org/blog/inpractice/video--how-to-remove-metadata-from-a-word-or-pdf-document/.

14. *Strengthen Passwords.* A weak password makes it easy for attackers to hack your account with password-cracking software. Once they have access to your accounts, they can steal other credentials to give them wider access to your system.
    a. Passphrases – Protect against this threat by strengthening all your passwords. Passwords should contain a minimum of 14 characters, including upper- and lowercase letters, numbers, and special characters. Use a passphrase to help you remember it. See this article for more information about strong passwords: https://www.osbplf.org/blog/inpractice/passphrases--an-enhanced-level-of-security/.
    b. Unique passwords – Make sure each password is unique. Don't reuse passwords for multiple devices or applications. Don't share passwords with anyone. Change passwords frequently, ideally every 30 days.
    c. Password manager – Consider a secure and reputable password manager like 1Password or Dashlane if you have too many passwords to manage.
    d. Multifactor authentication – Enable multifactor authentication. Your password is a single factor for authentication. Adding other factors makes your account more secure, such as a code texted to your cell phone or a biometric identifier like your retinal scan or fingerprint. See this article for more information: https://www.osbplf.org/blog/inpractice/safeguard-data-with-two-factor-authentication/.
15. *Train Staff and Create Policies.* Staff can put a firm at risk if they are not familiar with various threats, risks, and security protocols to protect client and firm data. Training and educating yourself and your staff is your first line of defense against a data breach.
    a. Staff training – Offer biannual or annual training so staff can learn the different ways security threats present themselves, including computer security, social engineering, identity verification, phishing and scams, and password management. The following companies offer employee cybersecurity training:
        i. Sensei Enterprises, Inc. (https://senseient.com/services/security-awareness-training/)
        ii. Inspired eLearning (https://inspiredelearning.com/)
        iii. KnowBe4 (https://www.knowbe4.com/)
        iv. Proofpoint (https://www.proofpoint.com/us)
    b. Periodic testing – If you're in a bigger firm, engage your IT person in educating staff about potential threats and the proper response.
    c. Security policies – Create written policies about encrypting devices, downloading software, vetting vendors, opening electronic files, working remotely, changing passwords, using work devices, engaging in social media at work, using email and the internet, etc. Here are sample policies to consider using: https://assets.osbplf.org/in_briefs_issues/Cybersecurity%20and%20Employee%20Training.pdf.

16. *Prepare an Incident Response Plan.* Part of your preparation for a data breach includes having a plan to respond to security incidents. An incident response plan (IRP) is comprised of steps a firm needs to take to manage the aftermath of an incident. An IRP can be a simple checklist or a comprehensive manual or handbook, depending on your firm's size, technology infrastructure, and business operation. If a data breach occurs, also see the PLF practice aid *What to Do After a Data Breach,* available on the PLF website, www.osbplf.org. Click on Services > CLEs & Resources > Practice Aids > Cybersecurity & Data Breach.
    a. Contact list – Include a contact list with each person's name, role, and contact information. The contact list should include the Professional Liability Fund (PLF), your cyber liability insurer (if different than the PLF), and your IT person.
    b. Response – Develop a process, with help from your IT person, to identify the scope of the incident, contain it, eradicate the source, and recover the affected systems.
    c. Review – Review the IRP at least once a year and make changes as needed.
17. *Purchase Cyber Liability Insurance Coverage.* Cyber liability insurance helps cover your firm's financial losses resulting from a data breach. Your PLF Primary Coverage Plan does not cover cyber claims, so consider purchasing cyber insurance—either through the PLF Excess Program or on the open commercial market with the help of an insurance broker. Your cyber coverage will vary depending on your plan. Typically, you will be provided with a breach response manager who will work with a team to determine how the breach occurred, how to contain it, whether clients should be notified, and any other necessary steps to protect you and your clients.

IMPORTANT NOTICES