Protecting Yourself and Your Law Firm from Data Breach Checklist

Data breach is the unintended exposure of your data to unauthorized viewers. As lawyers, we are entrusted with confidential data about our clients. This checklist is intended to help you to become more secure. Think of it as a cyber security checklist that is helpful for identifying areas of concern for you to discuss with your IT support person. As cyber security is an area of ongoing change due to the increasing sophistication of cyber criminals, you should continue to seek information about data security.

Passwords

1. Use passwords to protect all devices connected to the internet. Create strong passwords at least 14 characters or more using upper and lower case letters, numbers, and special characters. Use a passphrase such as a sentence to help you to remember it.

2. Use a password manager program to store your passwords securely in an encrypted vault on your computer or in the cloud. Don't store passwords in files on your computer such as in a Word document or Excel spreadsheet. If you must write down your passwords, secure it in a locked location.

3. Use two-factor authentication, which allows you to verify your identity using two methods of the following: **something you know** (for example a password), **something you have** (for example a key or hardware authentication device) **something you are** (for example a fingerprint or retina scan). Authentication devices provide strong two-factor authentication. For example, a YubiKey www.yubico.com itself is a two-factor authentication device incorporating a physical key with your fingerprint that plugs into your USB drive and supports one-passwords, public key encryption, and authentication. The YubiKey 4C Nano is the world's smallest USB-C authentication device for use with USB-C ports.

4. Keep your password confidential. Don't share it with anyone.

5. Keep your password unique. Don't re-use important passwords for multiple websites, devices, or services.

6. Change your password frequently, such as every 30 or 45 days. Don't recycle passwords!

Hardware and Software

7. Keep your hardware and software current with upgrades from the vendor. Those upgrades will typically include improved security features.

8. Secure your server in a locked room. Some cyber criminals have walked through law firms with clipboards posing as IT service personnel. Verify identities before granting access to your server.

9. Use intrusion detection systems. These systems will alert you to attempts to invade your computer system.

10. Use security software suites that include virus and malware protection and keep them up-to-date.

11. Have your IT support person set up your wireless network to include enabling strong encryption. Disable the WEP and WPA encryption and require WPA2 encyption.

12. Change the default passwords on all wireless routers and servers. Consult your IT support person for any help.

13. Be sure that any device holding client data is password protected and encrypted, especially if these devices are taken off site. Thumb drives, smart phones, tablets, and laptops continue to be most frequently stolen or lost devices.

Protocols

14. Back up all data and do regular periodic test restores of the backup. Store your backup securely. Backups taken off site or stored on the internet should be encrypted. If you are storing your backup or any data on the internet, be sure that the vendor does not have access to the decryption key.

15. Be sure that your IT support person sets up your backup system so it cannot be corrupted if your computer is attacked by ransomware. Otherwise, ransomware can travel onto your backup.

16. Develop a protocol for internet usage at work. Employees should not be allowed to download and install programs and apps on devices that connect to your server without prior authorization from your IT support person. Freeware frequently is infected with malware. Train your staff to avoid downloading any attachments sent by email especially if the extension ends in .exe which means it is an executable file.

17. Insure that all remote access to the office network occur through a VPN, MiFi, smartphone hotspot, or some other encrypted connection. Prohibit connecting to the office network using a public computer (such as at a hotel or library) and unsecured open public Wi-Fi network (such as at an airport, hotel, coffee shop, or library). Obtain guidance from your IT support person for setting up a VPN, MiFi, or smartphone hotspot.

18. Do not allow non-employees to have access to your network. This especially includes terminated employees.

19. Conduct an annual internal network security audit to ensure your network is secure. This is most helpful when it includes a vulnerability assessment.

Education

20. Provide mandatory social engineering awareness training to your staff annually.

21. Provide training to staff for how to respond to a cyber breach incident, including disconnecting the device from the internet and office network immediately if staff suspects the device has been breached and contact IT support immediately.

22. Instruct staff on how to properly dispose of any device or digital media that contains client or law firm data.

23. Instruct staff on proper safeguards if they are allowed to use their own device on your network.

24. Instruct staff on how to scrub documents for metadata.

25. Teach staff how to recognize phishing scams.

26. Teach staff to exercise caution on using social media as cyber criminals could use the same information to assist them in personal identity theft or hacking online accounts.

Resources for Further Study

27. "Back to Basics: 10 Security Best Practices," DARKReading, Nimmy Reichenberg, September 4, 2015 https://www.darkreading.com/operations/back-to-basics-10-security-best-practices/a/d-id/1322053

28. "Data Security," Federal Trade Commission. https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security

29. Lawyers Mutual Liability Insurance Company of North Carolina Data Breach Incident Response Plan Toolkit. http://files.www.lawyersmutualnc.com/risk-management-resources/risk-management-handouts/Data_Breach_Toolkit.pdf

30. "Protecting yourself from cybercrime dangers: The steps you need to take," by Tim Lemieux, December 1, 2013, Practice PRO. http://www.practicepro.ca/2013/12/protecting-yourself-from-cybercrime-dangers-the-steps-you-need-to-take/

31. Schneier on Security: Books by Bruce Schneier https://www.schneier.com/books/

IMPORTANT NOTICES

This material is provided for informational purposes only and does not establish, report, or create the standard of care for attorneys in Oregon, nor does it represent a complete analysis of the topics presented. Readers should conduct their own appropriate legal research. The information presented does not represent legal advice. This information may not be republished, sold, or used in any other form without the written consent of the Oregon State Bar Professional Liability Fund, except that permission is granted for Oregon lawyers to use and modify these materials for use in their own practices.