Law Firm Tips: Four Tips for Improving Database Security within your Legal Practice

How secure is your law firm's database? As a legal professional entrusted with your client's valuable information, you have an ethical duty to protect client data… so, cybersecurity should have a consistent spot at the top of your worry list. Hackers never take a break from their efforts to breach databases and steal data. So, your firm cannot afford to take a break from cybersecurity. Below are four tips for improving database security within your legal practice.

1. **Firm-wide Security Policies**

To implement a system of effective cybersecurity within your law office, you must first establish and implement policies that effectively address potential threats. These policies provide a roadmap for what you want you to want to accomplish with your firm's security and how to get there. They also communicate your expectations to staff members and let them know that you are serious about promoting cybersecurity within the firm.

Some common examples of useful security policies include:

- **Two-Factor Authentication –** Two-factor authentication works to prevent hackers from accessing your email or database systems even if they have already cracked your password. This technology uses a smartphone or other device to ensure that anyone accessing the system is actually authorized to do so.
- **Strong Passwords –** Hackers are constantly looking to bypass weak passwords. A password policy can thwart these efforts by requiring the use of strong, more difficult to crack, passwords for all firm related systems. You should also require password changes on a regular basis and encourage the use of different passwords for different systems. If

you're concerned about forgotten passwords, consider using a password manager to keep track of them all.

- **Email Policy –** Have you ever considered how many documents come in and out of your firm by email every day? Each of these communications is a new opportunity for a hacker, particularly if you are still using an unsecured, unencrypted email system. By implementing an email policy within your firm, you can at least minimize some of the risks. For internal communications within the office, require staff members to use a secure internal channel. In addition, a Client Portal, like the one offered through TimeSolv, adds a layer of protection to client communications. Clients can log into their individual accounts to securely access information about their cases and communications from the firm.
- **Personal Device Policy –** The growing mobility of legal practice has made the use of personal devices almost inevitable. Lawyers often use their personal computers and smartphones to access firm related systems and data, which can create a potential security risk. With a standard Bring Your Own Device (BYOD) policy, you can set parameters for the use of personal devices and educate your employees on how to properly secure their devices, whether they are working in the office conference room or on the couch at home.

2. **Regular Updates**

Are you one of those people who go years without updating their software and computer programs? If you are, you could be putting your data, as well as your client's information, at risk. Software updates can be useful in preventing cyber attacks because they come with improvements to various aspects of performance, including security.

As explained by Norton, software updates fix bugs within the program and patch the security vulnerabilities that hackers tend to target. Updates are about identifying issues and making necessary adjustments. They can add new useful features to your system and remove potentially harmful outdated ones.

I know it can be time-consuming to install some system upgrades, but think about how much more time consuming it is to try and clean up after a cyber attack. A few minutes of inconvenience now can save you from a substantial

headache later, so make sure that you are consistently using the latest versions for all of your software and devices.

3. **Encryption**

Law firms routinely manage extremely large amounts of data at any given time. Encryption is one method of keeping that information safe and secure. This technology works by converting data into unreadable code that is extremely difficult to decipher without access to an authorization key or password. It ensures that all access points to data are locked and inaccessible to unauthorized entities.

Encryption is an extremely useful security measure, working to protect data regardless of where it is stored. I don't have to tell you about the risk of laptops being lost or stolen. It only takes a minute in the wrong hands for sensitive data to be accessed, changed, or even deleted forever.

With encryption, you can protect the integrity of your data regardless of where your device ends up.

With a firm-wide policy on encryption controls, you can create a system that automatically encrypts data based on preset classifications. That way, you don't even have to rely on staff members during the encryption process.

4. **Employee Training**

Any policy is only as good as its implementation and enforcement, which starts with making sure that your employees are well informed and trained. Develop a comprehensive training program so that all staff members understand your cybersecurity policies and the part they should play in securing firm and client data. Your employees are the first line of security for your law office and a few hours of training can be the key to effective prevention. If you aren't sure where to start, there are numerous cybersecurity training resources on the internet or consider bringing in a consultant.

Remember that your law firm's security measures are not only about you. You have a responsibility to your clients to keep their information as safe and secure as possible at all times. If you haven't given your database safety a serious consideration, don't waste any more time. Implement these four strategies to get your security systems in line.

About Erika Winston:

Erika Winston is a freelance writer with a passion for law. Through her business, The Legal Writing Studio, she helps legal professionals deliver effective written messages. Erika is a regular contributor to TimeSolv and a variety of other publications.