Seven Signs that your Law Firm Isn't Taking Data Protection Seriously Enough

With all of the warnings and horror stories about cyber attacks and law firm vulnerabilities, it's hard to believe that some lawyers still haven't taken adequate measures to protect client information. By not doing so, these legal practices may be leaving the door open for the infiltration of their systems and serious data breaches.

If you aren't sure whether you fall into this category, here are seven signs that your law firm isn't taking data protection seriously enough:

Sign #1: You can't remember the last time you updated your software

If you have no idea how long it's been since you updated the software in your office, then you probably aren't thinking enough about data security. Outdated computer applications often lack the security measures necessary to handle current threats.

When software developers create updates, they do so with the intention of addressing shortcomings within the program, as well as newly identified threats. Updates keep software running correctly while addressing security vulnerabilities that can be exploited by hackers. But these updates can't work if you don't actually use them – and many attorneys fail to ever install them.

Outdated software creates a significant threat for your firm and the client data you possess. Without updates, you are placing your entire law firm system in jeopardy.

Sign #2: You've already been attacked

If your law firm recently experienced a virus or ransomware breach, you've already felt the consequences of not taking data protection seriously. Consider getting a security audit done as quickly as possible. An auditor can identify the weaknesses that led to system vulnerabilities and help you choose the best strategies for addressing them.

Don't assume that a previous attack makes you less likely to suffer a second one. If you fail to adequately address the problem in a timely manner, the source of the problem may still exist, essentially opening a door for hackers.

An earlier attack means that someone already dropped the ball on data protection. You don't want that to happen again.

Sign #3: You do the bare minimum

When it comes to protecting law firm data, general compliance may not be enough. Hackers understand these minimal requirements and they have spent an extensive amount of time creating strategies to infiltrate them.

Some of the information stored by law firms is even more sensitive than the financial data hackers seek from big businesses, so more care and attention must be given to keep it safe from a breach – and simple compliance just isn't sufficient. That fact that widespread breaches continue to happen begs the question whether minimum requirements go far enough.

As reported in an ABA Law Journal article, "Cybersecurity no longer can be relegated to the IT department or be part of general guidelines on computer use." Make sure that your law firm is taking the steps necessary to meet your ethical obligation of protecting client information and not just doing the bare minimum.

Sign #4: Your staff hasn't been trained

If every member of your law firm staff has not received security measures training, you may not be taking your data protection seriously enough. Human error is the most common culprit when it comes to data breaches. While many law firms spend an extensive amount of time and energy training staff members on how to best serve their clients, they often fail to provide adequate data protection training.

From learning about the importance of strong passwords to identifying potential email and physical threats, every lawyer, paralegal, and admin assistant in your firm plays a part in keeping your firm data protected and secure.

Sign #5: Your office isn't disaster ready

You never know when a disaster will strike. From an electrical fire to a weather-related event, your entire system can be devastated in a matter of minutes. When disasters happen, law firms can experience problems with the delivery of client services, protecting client information, and keeping sensitive data confidential.

The ABA recently published advisories to help law firms prepare for unexpected disasters. They suggest that lawyers create a readiness plan and also develop a business continuity plan. A disaster could occur at any moment, so serious data protection needs to include getting your office disaster ready.

Sign #6: Where did that new program and toolbar come from

New software and files unexpectedly popping up on your computer? These little surprises could signal a computer breach. A staff member may have installed legitimate software that happened to be tainted or opened a harmful email attachment.

Before you even realize it, your system has new software that may be transmitting valuable data to an unauthorized third party. The same goes for new toolbars. Hackers use these harmless-looking tools to install malware, redirect your internet searches, and breach your law firm systems. Pop-up software and toolbars should be taken seriously and addressed quickly.

Sign #7: Your system defenses are down

Your system automatically comes with various instruments for protection. Tools like Task Manager, Registry Editor, System Restore, and Safe Mode rebooting. When hackers attack, they often go after these tools first, with the purpose of stripping away your ability to make fixes. If any of these systems start acting erratically or fail to open all together, it could be a sign of trouble.

Disabled firewalls also result from inadequate data protection. Staff members may disable your system firewalls because they believe software will work better. While they think their actions improve their workflow, they are actually placing your systems and data in serious jeopardy. If your law firm doesn't have a firewall policy, you may need to rethink your data security.

It's not hard to find evidence of law firm cyberattacks and data breaches. As an effective attorney, you must take measures to protect your client information in a meaningful way. If any of these signs sound familiar, it is imperative to start taking your firm's data protection more seriously.