Is your office secure? A checklist for law firm cybersecurity

We continue to live in a world plagued by cybersecurity threats and data breaches. Though company breaches may not place at the top of our ever-changing news cycle anymore, they do continue to happen at an alarming rate. Security experts agree that breaches are inevitable, even for smaller companies, and that it's only a matter of time before your law firm is faced with a cybersecurity threat. Now, I know this sounds extremely grim, but it's vital that you understand the magnitude of what your legal practice is facing and the importance of preparation. This post seeks to provide you with some industry advice about policies and programs that you can implement to prevent a serious security hack and/or properly respond when one occurs.

Doing nothing is no longer an option

A disturbing number of law firms have been hacked over the past five years. From huge mega-firms to much smaller practices, hackers recognize two things about law offices:

1. The presence of valuable data – Law firms often store their clients' most sensitive data. From financial records to social security numbers and banking information, a law office computer is a hotbed of confidential information.
2. Lack of security measures – Even with all of the ominous reports and ABA opinions on the matter, many small and midsized law firms have yet to implement any effective cybersecurity policies… and hackers know it.

So, you combine valuable data with lacking prevention and what do you get? An open invitation for hackers to breach your law firm computers.

While most of the large and mega-sized law firms have the resources to maintain an in-house security team, this is a luxury that many small and midsized firms simply cannot afford. But that's still not an excuse to do nothing. According to the ABA, roughly 25% of law firms with 100–500+ employees have been breached. For firms with 2-99 employees, the range is about 14%. Those statistics are not insignificant, particularly when you consider that the average cost of a single data breach is reportedly around $200,000. Could your firm stand to lose a couple of hundred thousand dollars? I didn't think so.

The checklist

The following checklist spells out the steps that even a solo practitioner can take in the face of looming cybersecurity threats. Look them over and assess whether your law office is doing all it can to keep client data secure.

Layer your data protection

Adequate data protection requires multiple layers of safety measures. Make sure that your security system includes the use of encryption and strong authentication measures to protect against unwelcome hackers. If all of this sounds like a foreign language to you, get some help. Contract a reputable security company to give your data systems an overhaul.

Create a culture of cybersecurity awareness

Many data breaches are either directly or indirectly related to human error or carelessness. Whether it involves a tablet left on a restaurant table or an easily-guessed password, there are numerous actions that your employees may be taking to increase your firm's likelihood of breach. You can work to prevent these circumstances by ensuring that your entire staff is educated about cybersecurity risks and properly trained on what they can due to minimize them. Even if you already

have numerous regulations and procedures in place, they are of little consequence if your staff is not following them. There are numerous small things you can do to cultivate a culture of awareness. Contract an expert to conduct training. Post reminders around the office about prevention measures. Communicate clear rules and regulations about the use of mobile devices for firm-related work.

Run breach readiness assessments

After putting cybersecurity measures in place, it's important to make sure that they are actually working as expected. Readiness drills can be a great resource for testing your security systems, as well as your office as a whole for reaction to a cyber threat. Find a reputable cybersecurity agency that can come in and simulate an attack within your firm. You might find that you and your staff are not nearly as ready as you thought you were.

Look to clients

This is particularly useful for firms with business clients. Your existing or potential clients may have their own cybersecurity requirements for working with your firm. They have a stake in ensuring that their data will be safe with you, so they put measures in place to protect themselves. By tailoring your security preventions to meet their requirements (especially those coming from multiple clients), you are also improving your law office data security. So, the next time a prospective client hits you with a list of cybersecurity prerequisites, strongly consider the potential benefits of complying.

Software Updates

How many times have you chosen the "Remind me later" option when a system update alert pops up on your screen? Just as hackers spend their time trying to develop new threats, most reputable software companies are busy trying to protect against them. That's why updates

can mean the crucial difference between a breach and stronger security measures. I know this can be an expense – With the exception of TimeSolv time tracking and legal billing, which I'll get to soon– but the potential cost of a breach can be far more costly.

Cyber risk insurance

You may have never heard of cyber risk insurance, but trust me – it's an actual thing. Remember what I said earlier. A cyber attack is virtually inevitable. From the federal government to mega financial institutions, even the most expensive and sophisticated cybersecurity preventions have been breached by scheming hackers. Therefore, it's just as important to prepare for an actual breach as it is to try and prevent one. Data breaches can result in extensive damage and disruption to your law firm. Look into cyber risk insurance and consider making the investment.

Choose your cloud storage vendors wisely

Cloud storage is consistently gaining traction within the legal community, but not all providers are created equally. You want the assurance that your law firm and client data will be protected with the highest levels of security protocol. TimeSolv recognizes the value in your law firm data. That's why they have consistently maintained a secure and highly available system. Click here to learn more about the cybersecurity protection that TImeSolv provides and use this checklist to protect your law firm from security breaches.

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.