3 Strategies To Improve Data Security for Law Firms

It’s no secret that data security for law firms is of the upmost importance. News stories explain that hackers see law firms as wealthy targets, and the larger the client you land, the more of a target you become.

The ABA TechReport shows most attacks are directed at small and medium sized firms.

- **27%** of attacks were directed at firms with *2 – 9 attorneys*
- **35%** of attacks were directed at firms with *10 – 49 attorneys*
- **33%** of attacks directed at firms with *50 – 99 attorneys*

As far as cybercriminals are concerned, small law firms are the low hanging fruit. They’re easy pickings for criminal opportunists looking for an easy payday.

- **Law firms have a treasure trove of data.** They have client, firm and customer data in the form of agreements, documents, contact details, insider information, and personal and financial documents.
- **Law firms have deep pockets.** Cybercriminals assume law firms have a significant amount of cash on hand in the form of hourly billings or cash in a

client's trust account.
- **Law firms are exposed and vulnerable.** The ABA report also shows that a little over a quarter of surveyed law firms have experienced a data breach.

Law firms act as indirect information brokers. They're expected to safeguard their client's business. Sure that's not your core business. You're focused on taking care of your client's legal matters. But that doesn't matter to these cybercriminals.

What Law Firms Can Do To Improve Data Security

As information brokers, law firms can take precautionary steps to ensure that the information in their possession — law firm *and* client data — stays in their possession.

A report from LogicForce had some surprising implications.

- **53%** didn't have a data breach response/recovery plan
- **77%** of firms didn't have cyber insurance
- **95%** of respondents were noncompliant with their own cyber policies
- **100%** were noncompliant with their client's policies

The vast majority of law firms are vulnerable to a data breach. That's obviously bad news for law firms. However, these vulnerabilities provide law firms with the clarity and direction they need. Let's take a look at some of the steps law firms can take to secure their data.

1. Create a cybersecurity policy

A cybersecurity policy outlines the systems, procedures needed to guard your data against attacks. This policy provides firm-wide direction outlining:

- **Roles and Responsibilities:** Outline who is responsible for various aspects of cybersecurity within the firm.
- **Access Controls:** Specify who has access to which data and under what circumstances.
- **Data Protection Measures:** Detail how your data will be protected, including encryption and other security measures.
- **Accountability:** Assign clear responsibility for protecting the firm's data.

- **Security Programs:** List the necessary security software (e.g., antivirus, firewall, and anti-exploit software) that need to be installed and maintained.
- **Update and Patch Management:** Describe the procedures for applying hardware and software updates to ensure all systems remain secure.
- **Data Backup Protocols:** Outline the methods and schedules for backing up data, including the location of backups and the frequency of these backups.

2. Move to the cloud

Many small to medium law firms face challenges in preparing for potential data breaches. This isn't due to any lack of effort or capability; it's often about resources and costs.

Building a robust in-house IT department can be expensive. Here's a glimpse of what you might need to spend on key roles:

Title/Role	Small	Medium	Enterprise
Network Operations Manager	$131,011	$146,434	$161,603
Network Administrator	$82,922	$91,686	$101,051
Help Desk Support Rep	$40,145	$49,506	$59,822
Installation and Maintenance Technician	$99,238	$118,461	$141,090
Total Cost for IT Staff	**$353,316**	**$406,087**	**$463,566**

These figures only cover salaries and don't account for benefits, bonuses, or other perks. Additionally, they don't include costs for:

- Laptops, mobile devices, and other hardware
- Software licenses and setup fees
- Regular data backups, maintenance, and archiving
- Internet and network services
- 24-hour support, including higher costs for on-call staff

These expenses make a compelling case for law firms to move their operations to the cloud. Cloud-based practice management software enables you to offload your network security to a trustworthy provider. Bill4Time, for example, maintains bank-grade security to keep law firm operations running smoothly and safely.

With cloud solutions, your provider handles security, data backups, and compliance requirements. They protect your firm from data breaches,

unauthorized access, accidents, and human errors. Cloud-based providers are responsible for maintaining high levels of security and ensuring your data is backed up regularly, helping to shield your firm from various risks.

3. Create a disaster response and data recovery plan

The ABA Legal Technology Survey Report also highlights some concerning statistics as law firms face constant threats of cyber-attacks:

- 29% of firms have conducted a full security assessment by a third party to identify and address vulnerabilities.
- 43% of law firms use online backup solutions such as cloud-based services for storing their data securely.
- 34% of firms have an incident response plan, a concerning drop from previous years.

To safeguard client data and maintain the integrity of your firm, it’s imperative to implement a comprehensive disaster response and data recovery plan. Here’s an outline to get you started:

- **Incident Response Team:** Identify key personnel responsible for handling cyber incidents.
- **Contact Lists:** Maintain updated contact information for internal teams and external partners.
- **Backup Procedures:** Outline how and when data backups will occur, including locations.
- **Data Restoration Steps:** Specify the steps for restoring data from backups in an emergency.
- **Communication Plan:** Establish protocols for informing clients and stakeholders about incidents.
- **Access Controls:** Define procedures for managing and restricting access to sensitive data.
- **Testing Schedule:** Regularly test your disaster recovery processes to ensure they are effective.
- **Legal and Compliance Guidelines:** Ensure adherence to legal requirements and ethical standards for data protection.

Including these elements in your disaster response and data recovery plan will help you swiftly address and recover from any cyber incident, safeguarding your firm’s data integrity and client trust.

Good Data Security Makes Your Law Firm a Hard Target

It’s important to be proactive when it comes to data security for law firms. Breaches occur everyday, but with the right tools and processes in place, your firm doesn’t have to fall victim to the next cybersecurity attack.

FREE TRIAL