

4 Preventable Sources of Data Leakage & Revenue Loss in Law Firms

You may not recognize it, but a distinct connection exists between the loss of law firm revenue and the loss of law firm data. Let me paint a picture...

A client receives an invoice from your firm. He challenges the amount of the invoice, demanding to see verifiable proof of work completed on his behalf. Unfortunately, when you go to pull the relevant data to send the client, you cannot locate it. You are left with no way to adequately justify your bill, wasted time, and lost revenue.

Can you see the connection? This post will examine some of the most common sources of data leakage within your law firm and how those leaks show up as negative ROI on your spread sheet.

Inadequate Time Tracking

One of the most important aspects of compensation for any law firm is time tracking. How can you bill for time spent on a matter when you have no clue how much time was actually spent?

For many firms, this is where the data leakage and lost revenue begin. Every minute spent on a matter that goes untracked represents lost data and lost revenue for your practice. The lost revenue is obvious. No tracking equals no compensation, and even small losses quickly add up to become larger financial problems.

What may not be so obvious is the loss of valuable data that occurs when law firms fail to follow sufficient time tracking processes. Information about billable activity, timekeeper performance, and even project management is lost with inadequate time tracking.

This is the type of data firm leaders need to analyze the wellbeing of the practice and plan for greater success in the future. The data lost by inadequate time tracking not only costs revenue now, it could also cost revenue for years to come.

Compromised Emails

Email represents a form of data loss that can prove extremely costly. Attorneys constantly send messages that include valuable client and firm data. When this data is lost, it can prove extremely troublesome for the entire firm.

Compromised emails happen for numerous reasons, including:

- Nonsecure networks where cyberhackers are able to intercept emails
- Privileged messages sent to the wrong recipient
- The mistaken use of the “reply all” option

This type of data leakage can create severe financial and professional risks. An email to the wrong recipient could jeopardize a case, bring your firm’s ethics into question, and leave your legal practice with significant revenue loss.

Humans make mistakes

Nobody’s perfect, including the attorneys and staff members within your firm. Human error is one of the most common causes of data loss – particularly within a law firm where multi-tasking and interruptions are part of the daily norm. Every time the telephone rings, it diverts attention away from the most important (and profitable) tasks of the day.

To further complicate matters, law firms expect staff members to accurately track their time in the midst of this constant back-and-forth... which can quickly turn into notes scribbled on the sides of legal pads and sticky notes strewn about the desk... or no tracking of time at all.

Without proper timekeeping systems in place, timekeepers may underestimate the amount of time spent on a task, leaving money on the table. They may also overestimate the amount of time they spent, opening the door to ethical concerns. They may even remember to write down the time spent but forget to record details about the task.

Remember the example from the beginning of this post – an angry client and no way to justify your firm's bill. Relying on human memory for accurate and complete time tracking is gambling with your law firm data and revenue.

Security Breaches

Security breaches represent another revenue leaking consequence of human error. Much like the potential risks of compromised emails, when employees fail to follow standard security procedures, they put your firm's data and revenue in danger.

Cybersecurity experts overwhelmingly point to staff members as your first line of defense against security breaches. Even simple steps like changing passwords on a regular basis can help guard against cyberthreats. When your staff members fail to follow these guidelines, you can end up with leaked data and lost revenue.

For example, despite firm policies prohibiting such, your paralegal uses "1234567" as her password into all of the firm's systems. A cyberhacker easily hacks into your office system, accessing financial information for all of your client matters. Now, your firm is left having to face angry clients, bar complaints, and tens of thousands of dollars in related expenses.

Inefficient administrative processes

Most law firms fail to track any time that is not billable, but this represents a major data loss and potential loss of revenue. The harsh reality is that most law firms have no clue how much potential revenue is lost to non-billable tasks because they have no data to measure it. As a result, they also lose out on opportunities to improve efficiency when handling activities that do not contribute to a client's legal representation, so more time can be spent on the billable tasks that increase revenue.

Failing to track all firm time can become an extremely costly data loss. Every law firm should collect data regarding the time spent on such responsibilities as human resources, accounting, and everyday administrative tasks.

Preventing Data Leakage to Increase Law Firm Revenue

Data leakage does not have to be a part of your law firm culture. With effective procedures and rules in place, you can prevent these data losses, while implementing strategies that increase firm revenue. Here are three tips for preventing data loss within your law firm:

1. Identify data losses – Take a good look at your practice to identify areas where data loss is occurring.
2. Implement cybersecurity processes – Make sure that employees create strong passwords and use secure networks when sending emails and sharing sensitive data.
3. Track all time – Whether its billable hours spent on a matter or non-billable administrative tasks, your staff members should be keeping track of all firm hours on a daily basis.