How to protect your law firm from insider threats

How to protect your law firm from insider threats

He stole from their clients.

A law firm employee stole the identities of 20 clients. Working with several accomplices, this employee went on a “theft spree,” stealing $170,000 in cash, expensive clothing, jewelry and an additional $31,000 from a local Neiman Marcus.

Think about that for a moment.

A law firm employee had direct access to sensitive client information and he made off with it before anyone noticed there was a problem.

Who are these insider threats?

It’s your employees.

Intel found insiders were responsible for 43 percent of data breaches. In a separate report, Experian stated:

“*66 percent of data protection leaders admit that employees are the weakest link in an enterprise’s security posture.*“

This sounds harsh, doesn’t it?

It’s easy to state that these threats are simply “*your employees*.” It’s accurate, but it’s also incomplete. When it comes to insider threats, there are two kinds.

1. **Malicious.** These employees willfully cause harm, destruction and chaos in your firm.
2. **Accidental.** These are employees who gain access due to negligence, carelessness or poor systems and procedures.

Why would these employees harm your firm?

According to Gallup and Steve Rasmussen, former CEO of Nationwide, your employees fall into one of two camps, patriots or mercenaries. Not because they want to be but because they *have to be*.

- **Patriots:** These employees are engaged. They’re true believers who love, admire and believe in your law firm. They protect their firm’s interests, and they expect their firm to do the same for them. *Patriots give value first* to receive value.
- **Mercenaries:** They’re self-absorbed, corporate climbers who are focused primarily on themselves. At best, these employees are not engaged. At worst, they’re disengaged saboteurs who work to destroy your firm. *Mercenaries demand value first* and give value minimally; firms have to pay to play.

Here’s why this is a problem.

Research from Gallup shows 34 percent of employees in the U.S. are engaged.

That’s good, right?

Absolutely, but it’s also hiding an unpleasant reality here; **53 percent** of employees are “*not engaged,*” meaning, work is *just a job*. Another **13 percent** are “*actively disengaged*” these are active saboteurs, seeking to punish or destroy their employers.

What does this have to do with insider threats?

It’s about risk. According to the Insider Threat Report, the biggest risk factor to businesses: *too many users with excessive access privileges*.

> Threats to your business

Is this true?

A recent study found 70 percent of IT managers surveyed “*know or believe that users (employees) have business (client) data in their own personal file-sharing accounts.*”

What a disaster!

Law firm employees have sensitive client data stored in their *personal* Dropbox accounts!

Yikes.

This data is accessible to both malicious and accidental insiders, meaning law firms are exposed and vulnerable by default. This is a situation that requires *immediate attention*.

Protecting your law firm from insider threats

There are a few straightforward methods you can use to minimize insider threats. It’s so obvious, so unoriginal, you may feel the urge to roll your eyes.

1. Use a proven hiring methodology like Topgrading to recruit, vet and retain all-star employees.
2. Take very good care of your employees (from their perspective).

This creates patriots.

Next, use a layered approach to guard against both internal and external threats.

Let’s take a look.

Layer #1: Encryption for all endpoints

What’s an endpoint? An endpoint, according to Webroot,

“*An endpoint is any device that is physically an endpoint on a network. Laptops, desktops, mobile phones, tablets, servers, and virtual environments can all be considered endpoints*.”

Encrypting endpoints helps to maintain compliance with data protection regulations. It also gives you control over data wherever the endpoint goes. If a disgruntled employee walks off with a laptop, you can remotely perform a crypto-erase on that laptop's hard drive next time the employee connects to the internet. Hardware encryption also can't be turned off locally, meaning that employees can't bypass security measures you put in place.

Fully-managed encryption can be achieved in a couple of different ways.

- **Self-Encrypting Drives (SEDs)** – a hardware solution that's combined with remote administration is secure, easy-to-use and cost-effective. The SED automatically encrypts *all data* written to a hard drive, providing complete protection for your data. Encryption takes place on the drive itself, so there's no performance loss.
- **Cloud-based Encryption Management** – this is a software solution that requires no on-site server maintenance. It works with encryption tools native to the operating system (e.g., Microsoft's BitLocker or FileVault). It's also an inexpensive, fast and easy way for organizations to comply with regulations and maintain security.
- **Native Encryption Management** – Think Microsoft's native encryption feature, BitLocker. It stores encryption keys in hardware, so it's a little bit more secure than software encryption alone, but not as complete as full hardware encryption like the SED. If your firm is looking for an inexpensive way to boost security, BitLocker is a great start. Combine it with remote administration for complete control over your data.

Layer #2: User rights and access management

According to the Ponemon Institute, 62 percent of business users report they're able to access company data they probably should not see.

It gets worse.

The study also uncovered that when employees accessed files or emails they weren't authorized to see, 43 percent of businesses didn't detect the misbehavior for a month or longer. This means owners, partners, associates and support teams shouldn't have the same user rights.

I'm talking about the principle of least privilege.

What does this mean?

Access is only allowed on a need to know basis.

There are a variety of user rights and access management tools. If you use cloud-based practice management tools like Bill4Time, you can use user rights management tools like LastPass Enterprise to manage who has access to what, when and under what conditions.

Here's a demo that explains their service and how it works.

It's simple and easy to use.

Layer #3: Data loss prevention tools

Effective endpoint protection can be an uphill battle. Protecting endpoints in your firm requires flexibility – comprehensive protection with no unnecessary restrictions or interruptions to your work. This is where data loss prevention tools (DLP tools) come into play.

Effective DLP Tools:

- Locates and maps sensitive your data
- Inspects, classifies, filters and blocks leakage of your sensitive content and data. It doesn't matter if the channel is email, IM, Web, external storage or printers
- Blocks or encrypts data transferred to external media and devices as well as block connections to unsecure wireless networks
- Immediately recognize security risks, identifying any device that's currently or historically connected to your endpoints
- Generate regulatory compliance reports and security log summaries

The ideal DLP tool provides your law firm with complete protection, protecting sensitive data-in-use, data-at-rest and data-in-transit, without sacrificing productivity.

Layer #4: Consistent and testable backups

In my previous post, I mentioned that Matthew Perry's law firm was attacked by cybercriminals **twice**. His law firm survived two ransomware attacks with no loss of data.

How did he do it?

He did it with consistent backups. Perry conducted regular backups of all files at pre-determined intervals. He made sure he had backups in several locations (e.g., offsite, onsite, archived, cold, etc.). Then, Perry tested his backups **daily**, verifying that:

1. The firm's data was encrypted
2. Firm data was backed up successfully
3. That files were uncorrupted and accessible at a moment's notice

It's no secret, it just requires discipline.

Many firms don't have backups in place; those that do, fail to test their backups as often as they should.

Layer #5: Employee training and education

Your employees are insiders; these insiders, under the right conditions, are threats to your firm.

How do you address that?

With consistent training. When combined with user rights and access management, employees can make good decisions regarding:

- The attachments that should or should not be opened.
- When to ask for help
- How to spot phishing, spam and malware attacks
- How to avoid common pitfalls

If your employees aren't aware of your expectations, they're obviously less likely to meet them.

Insiders threats create data breaches

Almost half of the data breaches firms experience come from insiders. Your employees are the weakest link in your firm's security protocols.

They don't have to be.

With a layered security plan and a bit of foresight, you can prevent accidental mishaps, corral malicious insiders and protect your data. You can reduce the risk your firm faces from the internal and external threats surrounding your law firm – no crime spree necessary.

FREE TRIAL