TECHNOLOGY TIMES

FEBRUARY 2026

Insider Tips to Make Your Business Run Faster, Easier and More Profitably

# WHY MOST LAW FIRMS TECH IMPROVEMENTS FAIL

## AND WHAT ACTUALLY WORKS


*Every Law Firm Reaches This Moment…*

At some point, every firm has that meeting where someone finally says,

*"We need to get our technology under control."*

And then reality kicks in.

- A client's emergency comes up.
- A court deadline shifts.
- Someone can't access the document they needed five minutes ago.

Suddenly, every good intention takes a back seat to whatever fire is burning the hottest.

Here's the uncomfortable truth:

*Most IT improvement efforts fail because they depend on willpower instead of systems.*

### Why Law Firms Quit

*(In Technology… and in Fitness)*

The fitness world has understood this for decades.

People don't abandon goals because they're lazy — they abandon them because the structure around the goal is weak.

And law firms aren't any different.

The failure points look nearly identical:

- Vague goals: "Get in shape" is as useless as "improve our IT."
- No accountability: If no one tracks progress, falling behind becomes normal.
- No expertise: When you don't know what works, you guess — and often guess wrong.
- Going it alone: Motivation fades, and crisis mode takes over.

*Sound familiar?*

Most firms carry unresolved technology issues for months — sometimes years:

- "We really need to improve our backups."
- "Our security probably needs attention."
- "Everything feels slow, but not broken."
- "We'll handle it when things calm down."

*(Spoiler: in a law firm, things never calm down.)*

These problems don't persist because leaders don't care.

They linger because attorneys lack the time, structure, and technical expertise to make meaningful, lasting improvements between client demands and court deadlines.

### What Actually Works:

The *"Personal Trainer"* Model for IT
People who succeed in fitness often hire a personal trainer —not because they can't work out, but because the system handles the heavy lifting.

A great IT partner works the exact same way, giving your firm:

- Built-in expertise instead of guesswork
- Accountability that doesn't fall on your attorneys or staff
- Consistency, even when your team is swamped
- Proactive problem-solving that prevents emergencies before they happen

### What This Looks Like in Real Life

Picture a 25-person law firm where nothing is technically "broken," but everything is… irritating.

Slow laptops.
Random outages.
Unexpected downtime.
And constant moments of, *"Does anyone know how this system works?"*

That frustration adds up — in lost time, lost focus, and lost billable hours.

### What Happened When They Finally Brought in a Real IT Partner

The moment the firm partnered with a proactive IT provider, everything shifted:

- Backups were **tested, repaired, and verified**
- Devices were **upgraded on a predictable replacement cycle**
- Security gaps were **identified and closed**
- Productivity improved because the technology finally supported the work instead of slowing it down

And here's the key point:

**None of this required the managing partner to become a tech expert.**

### The One Decision That Changes Everything

If your firm chooses just one technology goal this year, make it this:

**Stop operating in firefighting mode.**

When your IT becomes predictable instead of chaotic:

- Your attorneys work faster
- Clients receive smoother, more reliable service
- You stop losing billable hours to preventable tech issues
- Growth becomes easier because your foundation is stable

This isn't about doing more.
It's about making your technology **reliable**—and not carrying that responsibility on your own.

ISMGRID

# 6 TECH HABITS

## YOUR FIRM SHOULD QUIT COLD TURKEY

Most law firms have a few tech habits everyone knows aren't great.

The risky shortcuts.

- The "we'll fix it later" processes.
- The workarounds that have quietly become *"just how we do things."*

They seem harmless — until the day they aren't.

If you want your firm's systems to run smoother, safer, and with fewer surprises, these are six tech habits worth quitting immediately… and what to do instead.

### Habit #1: Clicking "Remind Me Later" on Updates

That tiny button has caused more operational damage to law firms than most cybercriminals ever could.

Updates exist to patch known vulnerabilities — the very flaws attackers actively hunt for.
But "later" turns into weeks or months, and during that time, your systems are exposed.

Some of the largest ransomware outbreaks in history spread because firms skipped updates that were already available.

**Quit it:**

Schedule updates to run after hours, or let your IT partner push them automatically.
*No interruptions. No risk window. No excuses.*

### Habit #2: Using the Same Password Everywhere

Even the strongest password becomes weak the second it's reused.

When a small website suffers a breach, attackers buy the stolen credentials and immediately try them across:
Email, Case management systems, Banking portals
Cloud storage, Remote access logins.

This technique — credential stuffing — works with alarming success, especially in professional services.

**Quit it:**

Use a password manager (like 1Password or LastPass) that creates and stores unique passwords for every system your firm uses.

Simple. Secure. Done.

### Habit #3: Sharing Passwords Over Email, Text, or Slack

*"Can you send me the login?"*

It feels harmless — but it's one of the most dangerous habits in a law firm.

The moment a password is typed into an email, text, Teams, Slack, or anywhere else, it becomes permanently stored in:

- Email inboxes
- Cloud backups
- Server logs
- Search histories
- Mobile devices

If any of those accounts are compromised, cybercriminals can simply search for the word *"password"* and harvest everything.

**Quit it:**

Use the secure sharing options built into password managers.
No passwords in writing. No permanent trail. No unnecessary risk.

### Habit #4: Giving Everyone Admin Access Because It's Easier

Someone needs to install software, so you give them admin rights *"just for now"*… and then never remove them.

Suddenly, half the firm has the ability to:

- Bypass security controls
- Install risky applications
- Delete important folders
- Make system-wide changes

If even one of those accounts is compromised, attackers instantly gain the same unrestricted access.

**Quit it:**

Follow the principle of least privilege.

Everyone gets exactly the access they need — nothing more.

### Habit #5: Letting Temporary Workarounds Become Permanent

A process breaks.
You invent a workaround to get through the day.
Somehow, that workaround becomes the "official" way of doing things.

But workarounds:

- Waste time
- Create inconsistent workflows
- Depend on employees remembering tricks instead of using real systems
- Fail during high-pressure moments when you need reliability most

For law firms, where accuracy and deadlines matter, these hidden friction points quietly drain productivity and increase the chance of errors.

### Habit #6: The One Spreadsheet Running Your Entire Firm

That massive Excel file with 12 tabs and mysterious formulas known only to two people?

That isn't a system — it's a single point of failure.
If the file becomes corrupted…

If the formulas break…

Or if the person who built it leaves the firm…
Your operations can grind to a halt.

For a law firm, that risk is far too high.

**Quit it:**

Document what the spreadsheet is actually being used for, then transition those functions into proper tools with:

- Backups
- Permissions
- Audit trails
- Scalability
- Cross-team accessibility

This protects your workflows and makes your processes sustainable long-term.

### Why These Habits Stick — And How to Break Them

Law firms don't keep bad tech habits because people are careless.

They keep them because they're busy.
A risky shortcut feels fast in the moment, and the consequences stay invisible… until suddenly they aren't.

The firms that finally fix these issues don't rely on willpower — they change their environment.

With the right IT partner:

- Password managers get deployed firm-wide
- Updates happen automatically
- Permissions are managed correctly
- Workarounds disappear
- Critical spreadsheets become real, secure systems

The right way becomes the easy way.

# YOUR LAW FIRMS TECH

## IS OVERDUE FOR AN ANNUAL PHYSICAL

### Most Firms Avoid IT Checkups Until Something Hurts

Most people postpone going to the doctor until there's pain.

Law firms behave the same way with their technology.
If systems seem fine, nothing is visibly broken, and everyone is buried in casework, it's easy to assume all is well.

But just like your health, the absence of symptoms does not mean everything is healthy.
The issues that bring firms to a standstill are usually the ones quietly hiding beneath the surface — until the day they explode.

So here's the uncomfortable question:

When was the last time your firm's technology received a true checkup?

Not a quick printer fix.
Not unboxing a new laptop.

A holistic, preventative assessment designed to uncover risks you don't realise are there.

Because in IT — just like in medicine — *"working"* and *"healthy"* are two very different things.

The *"I Feel Fine"* Trap

Technology rarely warns you before something serious goes wrong.

Your systems can run smoothly for months while hiding major issues, such as:

- Backups that exist but cannot be restored
- Ageing hardware well beyond safe or reliable use
- User access that hasn't been reviewed or restricted in years
- Security gaps no one has detected yet
- Compliance requirements are silently going unmet

Your technology can appear functional… right up until the day one hidden issue becomes the worst outage your firm has ever faced.

### What a Real Tech Physical Examines

A proper technology assessment functions exactly like a medical physical: systematic, thorough, and designed to catch problems early — before they become emergencies.

### Backup & Recovery

This is the heartbeat of your firm's entire technology ecosystem.

If everything else fails, can you recover?

- Are your backups actually completing — not just scheduled?
- When was the last time you tested a full restore?
- If your server died on a Monday morning, how soon could your team be operational again?

Most law firms only discover their backups are broken during an emergency, and that is the absolute worst time to find out something isn't working.

Hardware & Infrastructure
Equipment ages quietly…until it doesn't.

- How old are your servers, firewalls, switches, and workstations?
- Is any equipment past manufacturer support (meaning no patches or security updates)?
- Are devices being replaced proactively, or only after they fail?

Downtime caused by ageing hardware is one of the highest hidden costs for law firms.

Systems run slowly for months — then fail suddenly, right when you need them most.
Access & Credentials

If you're unsure who has access to what, you're not alone — but you are at risk.

- Can you produce a complete, accurate list of current users?
- Are any former employees' accounts still active?
- Are shared logins hiding who did what and when?

For law firms handling sensitive client data, unclear access control is more than an inconvenience — it's a liability.

*...continued on page 4*

**SHINY NEW GADGET OF THE MONTH**

### Ember Temperature Control Smart Mug 2

The Ember Mug 2 isn't just a mug; it's your best friend during long, busy meetings. Set your perfect temperature in the app and keep it steady for 90 minutes, so every sip stays warm. Hand-wash safe and fully submersible, it's the ultimate upgrade for busy coffee lovers who love tech.

**CLIENT REVIEW**

### Leodean Worrell

"The speed with which ISM Grid address our firm's issues is outstanding. What is even more outstanding is the fact that their interface allows for very few calls being made to them. Finally, the fact that they provide us with weekly cybersecurity tips is impressive."

*Thank you so much for taking the time to share this feedback. We truly appreciate your kind words.*

*Providing fast, reliable support while minimising disruptions is exactly what we strive for, so it's great to hear that our systems and processes are working well for your firm. We're also glad you find value in our weekly cybersecurity tips — staying informed is a key part of protecting your practice and your clients.*

*Thank you for trusting ISM Grid with your IT and cybersecurity needs. We look forward to continuing to support your firm.*

## FREE REPORT

### The Legal Firm IT Playbook Every Managing Partner Should Have

Choosing the right IT partner shouldn't feel like guesswork — especially when your firm's billable time, client confidentiality, and reputation are on the line.
That's why we created The Legal Firm Owner's Playbook to IT Solutions, Services, and Fees — a free, practical guide designed to help attorneys make smarter technology decisions with confidence.


Inside, you'll learn:

- How to evaluate an IT partner's true security capabilities
- What services your firm should be getting (and what's often missing)
- How to avoid surprise fees, downtime, and vendors who don't understand legal workflows
- What a modern, well-managed IT environment looks like for a law firm
- The red flags that signal it's time to change providers

If you want technology that protects your firm, respects your billable hours, and gives you an edge in a competitive legal market, this guide is a must-read.

**Download your free copy of the Legal Firm IT Playbook and make your next IT decision your smartest one yet.**

## CARTOON OF THE MONTH


*...continued from page 3*

**Disaster Readiness**

Nobody enjoys thinking about worst-case scenarios, but avoiding them is what makes firms vulnerable.

Ask yourself:

- If ransomware struck tonight, what is your actual recovery plan?
- Is it written down — not just stored in someone's head?
- Has it been tested?
- Does more than one person know how to execute it?
- How long could your firm operate without access to systems or case files?

If your disaster plan sounds like, *"We'll figure it out,"* Then you don't have a plan.

### Compliance & Industry Requirements

In the legal world, *"healthy IT"* has a very specific definition — and regulators expect you to meet it.

Your firm may be required to follow:

- HIPAA, if you handle protected health information
- PCI, if you process or store credit card data
- Court, client, or insurance-driven cybersecurity requirements
- Contractual obligations in matters involving sensitive data

Compliance isn't optional — and it isn't just paperwork.

It's directly tied to client trust, professional ethics, and malpractice exposure.

Many Client Contracts Now Require Cybersecurity Controls.
More and more client agreements — especially in litigation, healthcare, financial services, and corporate matters — now include explicit cybersecurity requirements your firm must meet.

Compliance isn't just paperwork.

It protects your firm from:

- Costly fines
- Lost clients or contracts
- Ethical exposure
- Legal liability

In other words: compliance protects your reputation just as much as your systems.

### Warning Signs Your Firm Is Overdue for an IT Checkup

If any of these sound familiar, it's time for a technology assessment:

- "I think our backups are working."
- "The server is old, but it still runs."
- "We probably have ex-employee accounts still active."
- "We have a disaster plan… somewhere."
- "If this person left, we'd be in real trouble."
- "We'd probably fail an audit, but nobody has asked yet."

These aren't small concerns.

They're symptoms of significant risk — operational, financial, ethical, and legal.

The Cost of Skipping the Checkup
A preventative review costs a few hours.
A major failure can cost days or weeks of downtime — and far more in lost trust and billable time.

Data Loss:

Losing client records, financial documents, discovery materials, or active case files can be catastrophic for a law firm. Recovery is slow, expensive, and sometimes impossible.

**Downtime:**
Every hour your systems are down means lost productivity, missed court deadlines, delayed filings, frustrated clients, and damaged trust.

**Compliance Failures:**
Regulatory penalties are steep — and enforcement is increasing across industries, especially for firms handling sensitive data.

**Ransomware:**
The average recovery cost for a small business has climbed well into six figures.

For a law firm, the reputational fallout can be even more devastating.
Prevention is quiet and inexpensive.

Recovery is loud and extremely costly.

### Why You Can't Perform Your Own Tech Physical

You wouldn't diagnose yourself with a guess and a stethoscope.

You'd go to a professional who understands what *"healthy"* actually looks like.

Technology works the same way.

You need someone who:

- Understands the standards for a firm of your size and practice areas.
- Recognises patterns, warning signs, and overlooked risks.
- Can identify issues you've normalised simply because you deal with them every day.

That's the shift that turns IT management from constant firefighting into predictable prevention — the way it should be for a modern law firm.