TECHNOLOGY TIMES

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

JAN 2026

CYBERSECURITY BLIND SPOTS:

THE RISKS YOU DON'T SEE BUT HACKERS DO

Every business leader knows cybersecurity matters — but the biggest risks usually aren't the dramatic, headline-making attacks. They're the quiet vulnerabilities hiding in plain sight.

Small gaps that seem harmless… until a cybercriminal uses them as an entry point.

- A missed software update.
- An old user account that was never disabled.
- A backup system that no one has tested in months.

These aren't small oversights — they're open doors.

Here are some of the most common blind spots, and how to close them before they become expensive problems:

1. Unpatched Systems

Every skipped update gives attackers an advantage. Hackers monitor patch cycles closely and actively exploit known vulnerabilities.

Fix: Automate patching and set alerts for any systems that fall behind.

2. Shadow IT & Unapproved Devices

Unauthorized apps, personal laptops, and unmanaged phones can introduce hidden malware that sits quietly until it's triggered.

Fix: Enforce clear app and device policies, and routinely scan your network for unfamiliar endpoints.

3. Over-Permissive Access

Too much access is a security nightmare. Hackers love compromised accounts with admin-level or unnecessary permissions.

Fix: Apply the principle of least privilege and audit access rights regularly.

Fix: Follow the principle of least privilege, require MFA on every account and review access levels on a consistent schedule.

4. Outdated Security Tools

Cyberthreats evolve every day. Older antivirus programs, firewalls, or intrusion detection tools simply can't keep up with modern attacks.

Fix: Review your security stack regularly and replace ageing or unsupported tools before they become liabilities.

5. Orphaned Accounts

Inactive accounts from former employees are one of the easiest entry points for attackers. If the credentials still work, cybercriminals will find them.

Fix: Automate offboarding so accounts are disabled immediately — no exceptions.

6. Misconfigured Firewalls

A firewall only protects you if it's configured correctly. Old rules, temporary access, and undocumented changes can create exploitable gaps.

Fix: Audit your firewall settings, document every change and remove permissions that are no longer needed.

7. Untested Backups

A backup is useless if it doesn't restore. Many businesses find out too late that their backups are corrupted, incomplete or months out of date.

Fix: Test your backups regularly so you know they'll work when you need them most.

Fix: Test backups quarterly and store them in secure, immutable storage so they can't be altered or encrypted by attackers.

8. Missing Security Monitoring

You can't protect what you can't see. Without centralised visibility across your systems, threats can slip in and operate undetected.

Fix: Implement continuous monitoring tools or partner with a trusted IT provider who can watch your environment around the clock.

9. Compliance Gaps

Regulations like GDPR, HIPAA, and industry-specific standards aren't just legal checkboxes — they're frameworks designed to strengthen your overall security posture.

Fix: Schedule regular compliance audits, close gaps quickly, and maintain up-to-date documentation.

The Bottom Line

Spotting cybersecurity blind spots is only step one.

The real impact comes from fixing them — fast. Start with the steps above, and you'll reinforce your firm's defences where it matters most, reducing risk and protecting your clients, your business, and your reputation.

ISMGRID

TECH TRENDS

YOUR BUSINESS SHOULD ACTUALLY PAY ATTENTION TO

Every year, the tech world makes dramatic predictions about the "next big thing." Before long, you're buried in buzzwords — AI, blockchain, metaverse, quantum something — with no real clarity on which trends actually help your business grow.

Here's the reality:

Most tech trends are marketing noise meant to sell consulting packages.

But hidden in that noise are a few real shifts that will influence how you operate.

Let's skip the hype and get straight to what matters.

Here are three trends worth paying attention to — and two you can safely ignore.

Trends Worth Your Attention

1. AI Built Into Tools You Already Use

AI is no longer a separate platform you need to master. It's being woven directly into the software your team uses every day:

- Your email draft replies automatically
- Your CRM writes follow-ups
- Your accounting software categorises expenses and flags inconsistencies

Why it matters:

You're not adopting brand-new tools — you're getting smarter versions of tools you already pay for. The question isn't "Should we adopt AI?" It's "Should we enable the AI features we already have access to?"

What to do:

When your existing software rolls out AI features, test them for two weeks. Some will be useless — but others may save your staff hours every month.

Time investment: Minimal — you're already using these tools.

2. Automation Without the Headache

Creating automations used to mean hiring a developer or learning complex software. Not anymore. Today's tools let you build workflows simply by describing what you want in plain English.

Example:

"When someone completes our contact form, add them to our spreadsheet, send a welcome email, and remind me to follow up in three days."

The AI handles the setup behind the scenes.

Why it matters:

Automation finally moves from *"We know we should do this, but we don't have time"* to *"We can build this in 20 minutes."*

What to do:

Pick one repetitive task your team handles every week.
Describe it to an automation tool and let the AI create the workflow.
Time investment: 20–30 minutes to set up your first automation.

3. Security Regulations Get Real

Cybersecurity is no longer just a smart business practice — it's becoming a legal requirement. States are rolling out stricter privacy laws, insurers are demanding specific security controls, and enforcement actions are on the rise.

Why it matters:

Lacking basic protections isn't just risky anymore — it can mean higher insurance premiums, denied claims, penalties, or potential legal exposure.

It's quickly becoming the equivalent of operating without business insurance.

A risk you simply can't afford.

What to do:

Focus on three essentials:

- Multi-factor authentication on every account
- Regular, testable data backups
- Clear written cybersecurity policies that your team actually follows

Time investment: Two to three hours to set up correctly.

Trends You Can Safely Ignore

1. The Metaverse for Business

Virtual reality meetings have been "the future of work" for nearly a decade. Headsets are still expensive, uncomfortable, and impractical for most organisations. Unless you work in architecture, engineering, or design, you can pass on this one.

What to do:

Nothing. If VR becomes useful for everyday business, you'll know — because your competitors will be using it and seeing results.

2. Accepting Crypto Payments

Crypto may seem modern and innovative, but it introduces tax complications, volatility, recordkeeping challenges, and higher processing fees. Unless your clients repeatedly request it, it's not worth the operational hassle.

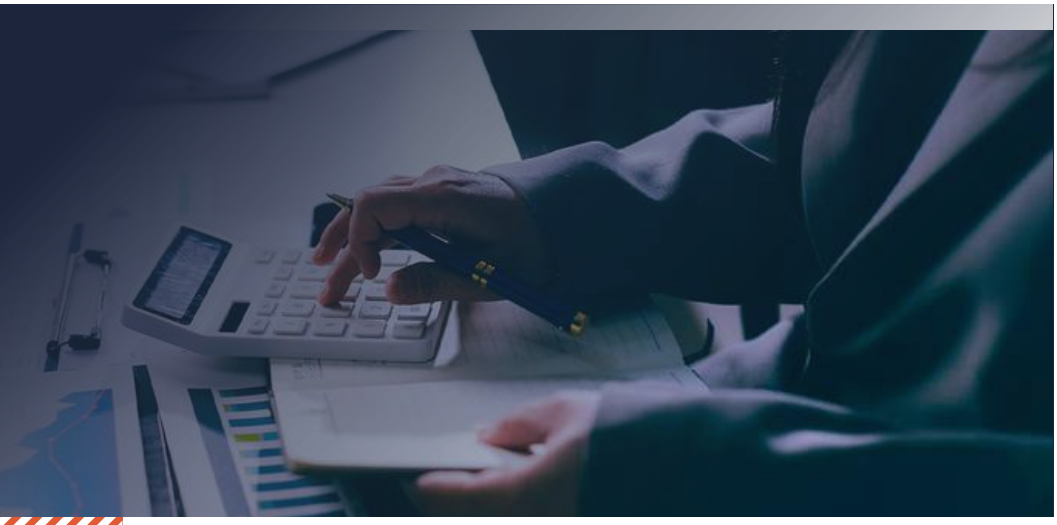
What to do:

If asked, politely decline. Revisit the option only if several clients begin requesting it on their own.

Final Takeaway

Prioritise technology that saves time, reduces risk, and improves efficiency.
Let the hype fade. Invest in the tools and trends that measurably strengthen your business — and skip the ones built on buzzwords.

THE HIDDEN COST OF IGNORING TECH HEALTH



Your business runs on technology, but when was the last time you checked its health?

IT maintenance often gets ignored until something breaks. The reality is that neglecting your tech environment doesn't just invite risk. It can quietly drain resources, reduce efficiency and erode trust over time. Regular IT health checks are as important as financial audits or employee reviews. They ensure your systems perform at their best and help you stay ready for the unexpected.

The high price of inaction

Neglecting the health of your technology ecosystem isn't a small oversight; it's a risk multiplier. When systems are left unchecked, small technical issues can grow into major disruptions. The longer these problems go unnoticed, the more expensive and complex they become to fix. Here are some of the hidden costs your organization could face when IT issues go unaddressed:

Financial costs

Downtime and lost revenue: Unidentified vulnerabilities or outdated infrastructure can lead to system outages, costing thousands per hour in lost productivity and sales. For businesses that rely on real-time transactions or customer-facing platforms, even a short outage can have a major impact. In competitive markets, downtime doesn't just halt work. It can also drive customers toward faster, more reliable competitors.

Ransomware and breach costs: Blind spots in your IT environment often become entry points for cyberattacks. The average cost of a data breach is now in the millions, and ransomware demands can cripple operations for days or even weeks. Beyond the immediate financial hit, there's the long-term cost of rebuilding systems, restoring data and regaining trust.

Compliance penalties: Missing controls, outdated policies or incomplete documentation can result in fines for noncompliance with HIPAA, GDPR or other regulations. These penalties can be severe and often come with a loss of credibility that affects partnerships and customer relationships.

Recovery and remediation expenses: Emergency fixes, forensic investigations and public relations damage control are far more expensive than proactive maintenance. A single breach can lead to legal fees, customer notifications, compensation claims and costly settlements. The more reactive your approach, the greater the long-term financial strain.

Security risks

Data loss or theft: Unsecured endpoints, outdated software or misconfigured access controls can expose sensitive data. Once data is compromised, recovery is difficult and customer confidence can take years to rebuild.

Unauthorized access: Orphaned accounts or unmonitored devices are often exploited by

...continued on page 4

SHINY NEW GADGET OF THE MONTH

OIKKEI AI Wireless Mouse

Meet the ultimate multitasker: a wireless mouse that doubles as an AI-powered audio recorder. Perfect for remote meetings, this device captures conversations accurately while you navigate your screen—no extra gadgets needed.

Streamline note-taking, improve collaboration and keep your workflow efficient. If you're looking for a simple way to save time and stay organized, this innovative tool is a game-changer for busy business leaders.

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

"The look you get when you say, 'Let's circle back.'"

...continued from page 3

accounts left active after an employee departs create opportunities for both external attackers and insider threats. These forgotten logins can sit unnoticed for months, giving cybercriminals an easy, ready-made entry point into your systems.

Malware Propagation

A single unpatched device can act as a launchpad for malware, allowing it to spread across your entire network. One compromised workstation can disrupt operations firm-wide and expose confidential data across multiple departments.

Operational and Strategic Impact

Reduced Performance

Outdated hardware and inefficient systems slow teams down, introduce workflow bottlenecks and frustrate users. When your technology becomes a barrier instead of a support system, productivity drops, morale declines and firmwide momentum suffers.

Missed Opportunities

If you don't have a clear understanding of your IT environment, strategic planning turns into guesswork. Without accurate visibility, it becomes difficult to forecast growth, budget for improvements or move forward confidently with digital transformation initiatives.

Falling behind on modernization doesn't just slow you down — it makes it harder to leverage new technologies effectively. Firms that avoid upgrading their systems risk losing ground to competitors who operate faster, smarter and with greater agility.

Poor Decision-Making

When leadership doesn't have accurate insight into IT performance, decisions become reactive instead of strategic. The result? Wasted budgets, misaligned priorities and preventable risks that slip through the cracks simply because no one could see them clearly.

Reputational Damage

Loss of Client Trust

A data breach or extended outage can undo years of credibility in a single moment. Clients expect reliability, confidentiality and professionalism. When those expectations aren't met, they won't hesitate to move to a firm that appears more secure and dependable.

Brand Impact

Public IT failures — whether outages, breaches or compliance lapses — can tarnish your firm's reputation and weaken your market position. Negative headlines and social backlash don't disappear quickly; the reputational impact can linger long after the technical issue is resolved.

Even after an issue is resolved, the damage can linger — overshadowing your firm's successes and shaking client confidence. Rebuilding that trust takes far longer than preventing the problem in the first place.

Ignoring your technology health doesn't just increase the risk of downtime.
It weakens the foundation your entire organization relies on.

Regular IT assessments help you:

- Identify vulnerabilities before they escalate
- Improve system performance and reliability
- Ensure compliance with evolving regulations
- Strengthen your security posture firm-wide

Think of it as preventive care for your business. A small investment in visibility and maintenance today can protect your reputation, reduce long-term costs and keep your organization operating smoothly for years to come.