RWK DIGITAL DISPATCH

JAN 2026

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

CYBERSECURITY BLIND SPOTS:

THE RISKS YOU DON'T SEE BUT HACKERS DO

Every business leader understands the importance of cybersecurity. Yet the biggest threats often aren't headline-grabbing breaches. They're the overlooked gaps hiding in plain sight. These blind spots may seem minor: a missed software update, an inactive account or an untested backup. But for hackers, they're open doors. Here are the most common gaps and how to close them before they become costly mistakes:

1. Unpatched systems

Every missed update is an invitation to attackers. Hackers track patch cycles and exploit known vulnerabilities.

Fix: Automate patch management and set alerts for lagging systems.

2. Shadow IT and rogue devices

Employees downloading unauthorized apps or connecting personal devices to your network can introduce malware that stays dormant until it's too late.

Fix: Enforce strict app and device policies. Regularly scan for unknown endpoints.

3. Over-permissive access

Too much access is dangerous. Hackers love accounts with excessive permissions.

Fix: Apply least privilege principles, mandate MFA and review permissions regularly.

4. Outdated security tools

Cyberthreats evolve daily. Old antivirus or intrusion detection tools can't keep up.

Fix: Audit your security stack and replace outdated tools before they fail you.

5. Orphaned accounts

Former employees' credentials often remain active, making them prime targets for attackers.

Fix: Automate offboarding to disable accounts immediately.

6. Misconfigured firewalls

A firewall is only as strong as its settings. Old or temporary rules create vulnerabilities.

Fix: Audit configurations, document changes and remove unnecessary permissions.

7. Untested backups

Backups aren't a safety net unless they work. Many businesses discover too late that theirs are corrupt or incomplete.

Fix: Test backups quarterly and store them securely in immutable storage.

8. Missing security monitoring

You can't protect what you can't see. Without centralized visibility, threats slip through unnoticed.

Fix: Invest in continuous monitoring or partner with an experienced IT provider.

9. Compliance gaps

Frameworks like GDPR or NIST aren't just paperwork. They're essential for strong security.

Fix: Conduct regular compliance reviews and maintain documentation.

Bottom line: Identifying blind spots is only the beginning. The real value lies in fixing them quickly. Start with these fixes and you'll strengthen your defenses where it matters most.

RWK IT SERVICES

TECH TRENDS

YOUR BUSINESS SHOULD ACTUALLY PAY ATTENTION TO

Every year, tech publications release bold predictions about revolutionary trends that will "change everything." Before long, you're buried in buzzwords such as AI, blockchain and the metaverse, with little clarity on what truly drives revenue growth.

Here's the truth: Most tech trends are hype designed to sell expensive consulting services, but buried in the noise are a few genuine shifts that will impact how you work. Let's focus on what really matters. Here are three trends worth your attention and two you can safely ignore.

Trends worth your attention

1. AI built into tools you already use

AI is no longer a separate tool you have to learn. It's being embedded directly into the software you already use every day. Your email program will draft responses. Your CRM will write follow-up messages. Your accounting software will automatically categorize expenses and flag any anomalies.

Why it matters: You're not learning new tools; you're just getting smarter versions of what you already use. Instead of asking "Should we adopt AI?" the question becomes "Should we turn on these features we're already paying for?"

What to do: When your software offers AI features, try them for two weeks before deciding if they help. Many will be gimmicky, but some will save hours.

Time investment: Minimal. You're already using these tools.

2. Automation without the headache

Building custom automations used to require hiring a developer or learning complex software. Now, new tools let you create workflows just by describing what you want in plain English.

Example: "When someone fills out my contact form, add them to my spreadsheet, send a welcome email and remind me to follow up in three days." The AI figures out how to make it happen.

Why it matters: Automation moves from "We should do this but don't have time" to "We can set this up in 20 minutes."

What to do: Identify one repetitive task your team does weekly. Describe it to an automation tool and see if AI can build it for you.

Time investment: 20 to 30 minutes to set up your first automation.

3. Security regulations get real

Cybersecurity is shifting from best practice to legal requirement. States are passing data privacy laws. Insurance companies are requiring specific security measures. Enforcement is getting serious.

Why it matters: Not having basic protections is becoming like not having business insurance. It's a liability you can't afford.

What to do: Cover three basics: multi-factor authentication on all accounts, regular data backups you can restore and written cybersecurity policies you follow.

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

Trends you can safely ignore

1. The metaverse for business

Virtual reality meetings have been "the next big thing" for a decade. Headsets are still expensive and uncomfortable. Unless you're in architecture or design, skip it.

What to do: Nothing. If VR becomes useful for mainstream business, you'll know because competitors will use it successfully.

2. Accepting crypto payments

Crypto sounds cutting edge, but it adds tax complexity, volatility and higher fees. Unless customers actively request it, stick to cards and ACH transfers.

What to do: If someone asks, politely say no. Reconsider only if multiple customers request it organically.

Focus on trends that save time, reduce risk and improve efficiency. Ignore the hype and invest where it truly benefits your business.

THREE "QUIET RISKS"

HIDING IN MOST IT ENVIRONMENTS

Your organization or municipality may already be paying for strong Microsoft security and modern productivity tools. The problem is… most of the real risk isn't a lack of technology. It's drift, oversharing, and impersonation that build up quietly over time.

Think of this like an annual physical. Bloodwork tells you what's happening inside, before you feel symptoms. The three programs below are designed to catch the "silent issues" that lead to outages, fraud, and uncomfortable conversations with leadership, auditors, or cyber insurance.

1) Microsoft 365 Security Governance & Enforcement

Analogy: Blood pressure management - set the baseline, then keep it in range.

Most organizations and municipalities don't get hit because they "have no security." They get hit because settings change, exceptions pile up, and one day you discover your environment has drifted.

What this solves

- Security settings that vary by department, location, or "who last touched it"
- Surprise changes that break access, weaken protection, or create gaps
- "We think it's set" without proof you can show leadership

How it helps

We establish a hardened Microsoft 365 baseline and continuously monitor for drift - so your environment doesn't slowly slide out of compliance. If something changes in the wrong direction, it gets caught early. If a rushed change causes issues, you can roll back to a known-good configuration.

A question to ask your team:

"If insurance asked us to prove our Microsoft 365 security settings are enforced, could we produce evidence quickly?"

2) Copilot Readiness & Secure Rollout

Analogy: Starting a powerful new medication, screen first, then dose carefully.

AI can save time. It can also surface information faster, which is great when permissions are clean… and risky when they aren't.

What this solves

- Leadership concern: "Will Copilot expose sensitive files internally?"
- Fear of paying for licenses without measurable ROI
- Lack of guardrails around what staff can do with AI and where data can go

How it helps

We run a Copilot readiness review (go/no-go), clean up the highest-risk gaps, and put governance guardrails in place. Then we roll out Copilot in a controlled pilot, starting with

…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.

POLICY CORNER:

AI Use at Work, Smart, Safe, and Clear

AI tools are showing up in every workplace… whether leadership approves them or not.

A simple AI Acceptable Use Policy helps you:

- Prevent sensitive data from being pasted into public AI tools
- Define what's allowed (and what's not)
- Keep teams productive without creating compliance risk
- Protect your organization if something goes wrong

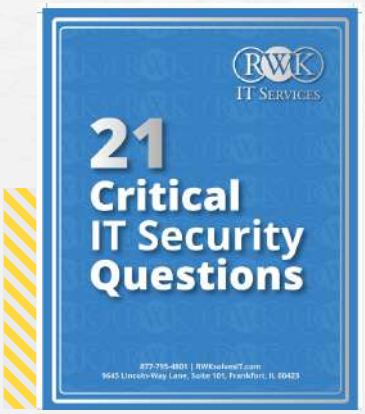
If you don't have an AI policy yet, we can help you create one that's short, clear, and enforceable.
Call: 877-795-4801

FREE REPORT

The Business Owners Guide To IT Support Services And Fees

You'll learn:

- The "dirty little secret" of the IT support industry that most people don't know and will never be told by their IT guy.
- 21 revealing questions that will help you instantly spot an unethical or grossly incompetent IT support technician in minutes.
- 4 most costly misconceptions most business owners have about IT services and what you need to consider when selecting an IT firm.
- Hackers, ransomware and data theft: what you REALLY need to know to protect yourself from a costly, devastating ransomware attack.



Download your FREE copy today at: www.RWKsolvesIT.com/21-Questions or call our office at (877) 795-4801.

CARTOON OF THE MONTH

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

...continued from page 3

departments most likely to see measurable value (Clerk, Finance, Admin, HR, Public Works, etc.) before expanding.

A question to ask your team:

"If someone asked Copilot to summarize sensitive content, are we confident only the right people would see the results?"

3) Email Domain Protection (Anti-Spoofing & Deliverability)

Analogy: A tamper-proof seal and verified signature on official organization and municipal mail.

One of the most damaging scams to organizations and municipalities isn't "hacking." It's impersonation, emails that look like they're from the Village, Finance, HR or leadership, sent to residents, customers or vendors.

What this solves:

- "Fake email" scams requesting payments, gift cards, invoice changes, payroll updates
- Customers. residents and vendors losing trust in official communications
- Legitimate emails landing in spam because authentication isn't aligned

How it helps

We implement email authentication and enforcement that tells receiving mail systems: "Only these systems are allowed to send as us, block the rest."

It also provides reporting so you can see every platform sending email on your behalf (billing, alerts, newsletters, permitting systems) and fix what's misconfigured—without breaking legitimate delivery.

A question to ask your team:

"Can someone spoof our domain today and send an email that looks like it came from our organization or village?"

Quick "self-check" (60 seconds) If you answer "not sure" to any of these, it's worth a review:

1. Do we have proof our Microsoft 365 security settings are enforced?
2. Are our file permissions and sharing controls clean enough for AI tools like Copilot?
3. Can criminals impersonate our domain in emails to clients, residents or vendors?

Next steps

If you'd like, we can run a short Security & Trust Review and give you a plain-language summary of:

- What's currently enforced vs. assumed
- The top 5 changes that reduce risk fastest
- A practical rollout path (including a safe Copilot pilot plan)