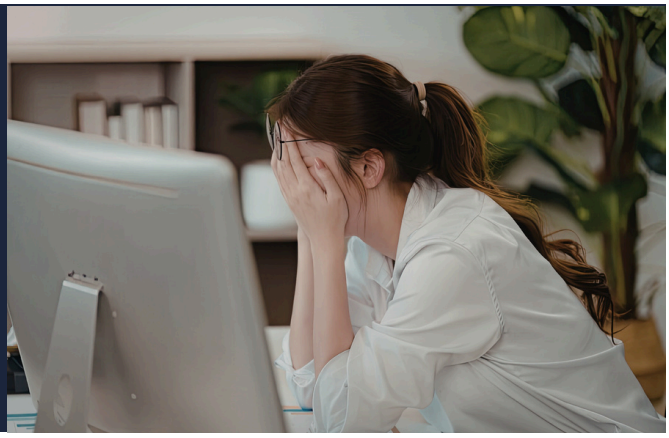
RWK DIGITAL DISPATCH

Cybersecurity & IT Tips for Local Government, Nonprofits & Growing Organizations

MARCH 2026

YOUR PEOPLE AREN'T THE PROBLEM

THE HIDDEN FRICTION SLOWING YOUR ORGANIZATION DOWN



Most teams are not underperforming. They are working around broken workflows.

That shows up in ways people start treating as normal: duplicate entry, approval delays, slow systems, shared logins, too many manual steps, and "temporary" fixes that never go away.

Over time, that friction gets expensive. It drains staff time, slows service, increases risk, and makes good people look less effective than they really are.

Here's the rule:

If work depends on a workaround, the system is the bottleneck.

Across municipalities, nonprofits, and growing organizations, that bottleneck usually shows up in three places:

1. Systems don't connect cleanly.

When systems don't share information, staff become the integration layer. That means duplicate entry, inconsistent records, and wasted time chasing the latest version. Over time, routine work becomes harder to track, standardize, and hand off.

2. Performance problems become accepted.

Slow Wi-Fi, lagging cloud apps, glitchy calls, and delayed file access rarely trigger a crisis, but they quietly reduce productivity every day.

3. Access and approvals are unmanaged.

When the wrong people have access, the right people are stuck waiting. That creates delays, risky workarounds, and single points of failure.

The fix is not more technology.
The fix is structure:

- better system alignment
- cleaner permissions
- stronger endpoint controls
- automation where it removes repeat work
- recovery and security processes that are actually tested

That's how organizations become faster, safer, and easier to run.

Ask yourself:

What does your team re-enter, wait on, or work around every day? That is usually where the real control gap is hiding.

Workaround test

If your team says any of these often, you likely have an operational friction problem:

- "I have to enter it twice."
- "Only one person can do that."
- "The system is slow again."
- "We'll fix it later."
- "Just use this for now."

How RWK helps

We reduce friction through system alignment, access control, automation, tested backup and recovery, and practical security guardrails.

We also help teams use OneNote with Copilot to turn meeting notes into action items, document procedures, and organize institutional knowledge so important information does not get lost or stay trapped with one person.

Used well, these tools make organizations faster and more consistent. Used without structure, they create risk, which is why AI needs guardrails.

Free Domain Trust Scan

See how protected your email domain is against spoofing and impersonation.

- Get your score in under 60 seconds
- See SPF, DKIM, and DMARC status
- Get a plain-English summary of what to fix first
- Scan the QR

or visit: rwksolvesit.com/domain-scan/

AI IS ALREADY IN YOUR ORGANIZATION

THE REAL QUESTION IS WHETHER IT HAS GUARDRAILS

Most organizations do not roll out AI. It rolls itself out.

Someone uses it to rewrite an email. Someone uses it to summarize meeting notes. Someone uses it to draft a policy, job description, or public-facing update. It saves time, so it spreads.

That is the opportunity. And the risk.

AI can absolutely help teams move faster. But it also makes bad information sound convincing, makes oversharing feel harmless, and creates a new shadow-technology problem: people using tools before leadership has decided what is acceptable.

What looks like an AI issue is usually a control problem underneath. In most organizations, the real gaps are unclear acceptable use rules, weak data-handling standards, inconsistent review expectations, and too much access to information that should be more tightly controlled.

RWK's position is simple:

AI is a productivity tool. It becomes a liability when rules are unclear.

This is not mainly a technology issue. It is a governance issue.

A practical AI policy should answer 4 things:

- Which AI tools are approved
- What data should never be entered
- What always requires human review
- What could create compliance or reputational risk

It should also answer two operational questions leaders often overlook:

- Who is responsible for monitoring how AI is being used?
- What happens when staff use AI outside approved guidelines?

You do not need a 30-page policy. You need rules people can use in the moment.

A good policy should reduce uncertainty, not create more of it. Staff should know what is allowed, what needs review, and where the boundaries are before a mistake happens.

Green / Yellow / Red

GREEN: Safe with normal care

Drafting routine internal content, formatting notes, summarizing non-sensitive information, brainstorming ideas, and improving readability on low-risk documents.

YELLOW: Use with review and judgment

Leadership-facing drafts, public communications, internal procedures, process guidance, board or committee materials, and anything that may become an official record.

RED: Do not put into public AI tools

Sensitive client, donor, employee, resident, financial, legal, HR, password, or security information.

Rule of thumb:

If the information is sensitive, regulated, confidential, or operationally risky, it does not belong in a public AI tool.

That includes more than obvious confidential data. It also includes information that could expose internal weaknesses, create confusion if it is wrong, or be misread without review.

This is especially important in Microsoft 365 environments. Copilot and similar tools do not just create content. They also surface information based on existing permissions. If access is overly broad, AI can expose files, emails, and data to the wrong people faster than leadership expects.

That is why AI governance has to include permission review, not just user guidance.

How RWK Helps

We help organizations put practical AI guardrails in place with AI acceptable use policies, data-handling rules, approval standards, Microsoft 365 and Copilot permission reviews, and clear guidance staff can actually use.

We evaluate, then act.

The goal is not to slow adoption down. It is to make sure speed does not come at the cost of judgment, accountability, or control.

RWK IT Services

THE CONTROLS MOST ORGANIZATIONS ARE MISSING

AND WHAT ACTUALLY REDUCES RISK

Most organizations believe they are covered.

They have antivirus, backups, a firewall, and a few policies. But the issue is rarely whether tools exist. It is whether controls are actually in place, enforced, and working together.

Risk does not come from what you bought. It comes from what is missing, inconsistent, or assumed.

Here are the areas where we most often see gaps:

Risk #1: Email Trust Is Not Fully Protected

Email is still the most common path for fraud, impersonation, and credential theft. Most organizations have spam filtering. Far fewer have real protection against domain spoofing.

That is a control problem, not just an email problem. If your domain can be impersonated, someone else can abuse your name and your credibility.

What to look for:

- Are you protected against domain impersonation?
- Do you know who can send email on behalf of your domain?
- Would your systems reject unauthorized senders?

Risk #2: Endpoints Are Not Consistent or Controlled

Laptops and desktops are where most work happens. They are also where inconsistency builds quietly.

Unapproved software, browser extensions, and leftover admin rights create risk and make environments harder to support. Endpoint security is about controlling what can run, not just hoping threats get caught later. RWK's framework is explicit on this point: endpoint security is about controlling execution, not just detection.

What to look for:

- Can users install software freely?
- Are admin rights tightly controlled?
- Do all devices follow the same standards?

Without endpoint control, security and performance both suffer.

Risk #3: Access Is Managed Informally

Access problems are rarely obvious until something breaks.

Too much access, not enough access, or the wrong access at the wrong time slows work and creates real exposure, especially during staff transitions. RWK's framework notes that access risk builds over time through excessive permissions and inconsistent controls, not just one-time mistakes.

What to look for:

- Do you know who has access to what, and why?
- Are shared accounts still being used?
- Is onboarding and offboarding handled consistently?

Access should be structured, not improvised.

...continued on page 4

CLIENT SPOTLIGHT:

RWK tailors their service to our specific needs instead of trying to fit us into a generic program. That's something we didn't get with other companies.

They've helped us implement multi-factor authentication, migrate our systems to the cloud, and strengthen the way our environment is managed overall. More importantly, they consistently bring ideas to the table that **help protect the township** and make it easier for our team to do their jobs.

As a government organization, we're held to specific standards and requirements. **Thanks to RWK, we're not just meeting those expectations, we're exceeding them.**

Working with RWK has allowed us to **operate more effectively** because they're in the background orchestrating our technology and **supporting our success.**

– Town Administrator, Illinois Township

FIELD CHECK OF THE MONTH

ZERO-TRUST APPLICATION CONTROL

Most incidents start small: an unapproved app install, a risky browser extension, or admin rights granted "temporarily" that never got removed.

Quick check: Who can install software today, and do you have an approved list?

How RWK helps: We help build zero-trust environments where only approved applications and essential processes are allowed to run, reducing exposure from risky software, unnecessary admin rights, and unauthorized changes.

...continued from page 3

Risk #4: Policies Exist But Don't Guide Behavior

Most organizations have policies. Fewer have policies people consistently follow.

When acceptable use, AI use, or security expectations are unclear, staff make judgment calls in the moment. That leads to inconsistency, not accountability.

A policy is only a control if it changes behavior.

What to look for:

- Do staff know what is allowed without asking?
- Are policies written for real decisions, not just compliance?
- Are expectations consistent across departments?

Risk #5: Backup Exists, But Recovery Is Assumed

Backups are often treated as a safety net. But in many environments, restore capability is untested.

That is a control gap. If you cannot reliably restore systems, data, and operations, backups create false confidence instead of real resilience.

What to look for:

- Have restores been tested recently?
- How long would recovery actually take?
- Who owns the recovery process?

Risk #6: Cyber Liability Requirements Are Not Verified

Insurance carriers are no longer accepting 'we have security in place' as an answer. They expect proof.

That turns controls into a leadership issue. It is not just about having safeguards, it is about being able to demonstrate them under pressure.

What to look for:

- Could you verify your controls if asked today?
- Are configurations documented and consistent?
- Do you know where your gaps are before someone else finds them?

Why This Matters To Leadership

These are not technical issues. They are operational risks. They affect time, risk, and accountability across the organization. When controls are unclear or inconsistent:

- staff lose time to workarounds
- decisions slow down
- risk increases quietly
- accountability becomes harder to prove

And when something goes wrong, leadership is left answering for systems they were told were "handled."

Quick Self-Check

- Can we prevent unauthorized use of our email domain?
- Do we control what software can run on our devices?
- Do we know who has access to what, and why?
- Are backups tested, or assumed to work?
- Are our policies clear enough to guide real decisions?
- Could we demonstrate our controls for cyber liability review?

If those answers are unclear, the issue is not visibility. **It is control.**

JEFF SPOKE AT IPAI

Jeff Reiter of RWK IT Services recently spoke at the Illinois Property Assessment Institute State Conference in Normal, Illinois, on March 23 and 24. His sessions focused on secure email, cloud systems, and AI risk in assessment offices, addressing the real technology issues assessors face today – from unsecured email and spoofing risk to uncontrolled AI use and data protection during appeal season.

COMMON GAPS WE SEE

"We thought we had that covered."

Most organizations don't have a technology problem.

They have a visibility problem. Controls are assumed, but not verified.

That's where risk lives.

NOT SURE WHERE YOU STAND?

START WITH A CONTROL REVIEW

Most organizations believe their controls are in place. Few have tested them under real conditions.

A short review identifies the few control gaps creating the most risk and operational friction.

What you get:

- Clear view of current control gaps
- Prioritized next steps
- Alignment between operations, security, and leadership expectations

RWK focuses on:

- domain authentication and spoofing protection
- Microsoft 365 configuration control
- Zero Trust access and endpoint enforcement
- AI acceptable use and Copilot permission risk
- incident response and recovery readiness
- documentation that supports cyber liability defensibility

Start with a conversation | RWKsolvesIT.com | 877-795-4801