RWK DIGITAL DISPATCH

FEBRUARY 2026

Cybersecurity & IT Tips for Local Government, Nonprofits & Teams Like Yours

WHY MOST IT "IMPROVEMENTS" FAIL (AND WHAT STICKS)

AND THE 30-DAY CADENCE THAT ACTUALLY STICKS

Every organization says they want "better security" and "less downtime." But in municipalities, districts, and nonprofits, urgent work always wins: a vendor needs access, a new hire needs a laptop, a system update gets delayed "until next week." The result isn't usually a big, dramatic failure, it's quiet risk:

- Shared logins that never got cleaned up
- "Temporary" admin rights that became permanent
- Backups running… but never tested
- Documentation missing when audit season hits

Here's what RWK sees working when the stakes are public service, trust, and continuity.

Why People Quit

The problem isn't effort, it's friction.
Most teams don't fail because they don't care. They fail because improvements require time, coordination, and follow-through… and no one owns the cadence.

Common "friction points" we see:

- "We'll patch after the next meeting / board session / shift change."
- "Only one person knows how this system works."
- "Vendor access is messy, but it's working."
- "We're not sure what 'good' looks like, or how to prove it."

What Actually Works: The 30-Day Cadence

The organizations that get ahead don't chase big projects. They run a simple, repeatable cadence that creates control, and proof.

Week 1: Patch and verify

- Confirm critical updates applied (servers and key endpoints)
- Review the exceptions list (what didn't patch and why)

Week 2: Access control

- Remove stale accounts and shared logins where possible
- Confirm MFA coverage on email, remote access and admin accounts

Week 3: Backup proof

- Perform one test restore (even a small one)
- Record the date and result (this becomes your "audit evidence")

Week 4: Incident readiness

- Confirm who does what if something looks suspicious
- Validate: "Can we shut off vendor access in 10 minutes?"

The goal isn't perfection. The goal is control you can defend.

What This Looks Like in Real Life

You don't need a 40-page "cyber program" collecting dust. You need operational control, and a team that keeps it current:

- Who has access (and why)
- How fast we can remove it
- How we recover if a system fails
- How we prove the basics were done (patching, backups, MFA)

When those answers are always ready, leadership feels it: fewer surprises, fewer fire drills, and confidence you can defend.

Examples we see most: CAD/RMS access, shared inboxes, utility billing, board/volunteer turnover, vendor logins, and "temporary" admin rights.

FREE: AUDIT-READY CHECK

If you're a municipality, district, nonprofit, or small business, RWK will provide a short, plain-English snapshot of:

- Access risks (stale users, vendor logins, admin rights)
- Email impersonation exposure (SPF/DKIM/DMARC)
- Backup readiness (including test-restore proof)
- The fastest fixes that reduce risk this month

https://rwksolvesit.com/discoverycall/

RWK IT Services

6 TECH HABITS

YOUR BUSINESS SHOULD QUIT COLD TURKEY

In every organization, whether you're a municipality, district, nonprofit, manufacturer, or professional firm, workarounds happen for a good reason: the mission can't pause. But the same shortcuts that keep things moving can quietly create audit gaps, downtime risk, and security exposure.

Here are six habits RWK sees most often, plus what to do instead.

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

Delaying updates feels harmless… until a known vulnerability becomes an entry point.

Quit it: treating patching like a best-effort task.
Do this instead: schedule a monthly patch window and keep a simple "patched / deferred / why" record.

How RWK helps: We run a maintenance cadence with reporting so leadership can see progress and exceptions

Habit #2: Using the Same Password Everywhere

Reused passwords still fuel credential stuffing attacks.

Quit it: "strong password" reuse across accounts.
Do this instead: use a password manager and require MFA on email, remote access, and admin accounts.

How RWK helps: We simplify secure sign-in standards so staff aren't fighting the process.

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

Shared credentials eliminate accountability and make offboarding messy.

Quit it: sending logins in email, texts, or spreadsheets.
Do this instead: store and share access through an approved vault, with access tracking and quick removal.

How RWK helps: We set up secure sharing that still works for shift-based and volunteer-heavy teams.

Habit #4: Email Impersonation "We'll Get to It Later"

If your domain protections aren't enforced, attackers can spoof your organization to staff, vendors, residents, and donors.

Quit it: assuming basic email settings are "good enough."
Do this instead: enforce domain authentication (SPF/DKIM/DMARC) and monitor for spoofing attempts.

How RWK helps: Our Email Impersonation Defense locks down your domain and gives you a clear "trust status" you can track over time.

Habit #5: Giving Everyone Admin Rights "Because It's Easier"

Admin rights are convenient, but expensive during incidents.

Quit it: local admin rights as the default.
Do this instead: least privilege and approved software list and IT-managed installs.

How RWK helps: Our Zero-Trust Application Control blocks unapproved/risky software and reduces admin rights without slowing teams down.

Habit #6: The One Spreadsheet Running Your Entire Business

Spreadsheets become mission-critical systems without permissions, logging, or reliable recovery.

Quit it: running key workflows on a file with no controls.
Do this instead: move critical workflows into permissioned systems with versioning, audit trails, and backup.

How RWK helps: We help teams migrate "critical spreadsheets" into tools that are controlled, recoverable, and defensible.

Why These Habits Stick and How to Break Them

These habits don't exist because people are careless, they exist because teams are busy and services can't stop.

The fix is a repeatable cadence plus two high-impact controls:

- Email Impersonation Defense (so your domain can't be used against you)
- Zero-Trust Application Control (so unauthorized software and admin sprawl don't become your next incident)

YOUR ORGANIZATION'S TECH

IS OVERDUE FOR AN ANNUAL CHECKUP

Most environments don't fail all at once. They drift. Access expands, exceptions stack up, and "temporary" shortcuts become permanent. Everything can look fine, until an audit request, a suspicious email, or a system failure forces the truth.

Here's the uncomfortable question: If something looked suspicious right now, would your team know exactly what to do first, and could you prove it later?

A yearly checkup turns "we think we're okay" into "here's the evidence."

The "I Feel Fine" Trap

Tech problems rarely announce themselves. They hide in places like:

- Backups that run, but haven't been tested
- Shared logins that erase accountability
- Old vendor accounts that still work
- Admin rights granted "just to get it done"
- Email impersonation exposure no one sees until it's used against you
- No clear incident steps, just "call someone and hope"

The risk isn't just security. It's downtime, reputation, and liability.

What a Real Tech Physical Examines

Not a 40-page binder. A practical review that shows what's solid, what's risky, and what to fix first.

Backup and Recovery

This is your heartbeat. If something fails, can you recover?

Ask:

- When was our last successful test restore?
- Which systems must come back first (email, finance, CAD/RMS, file systems)?
- If Monday morning goes sideways, how long until we're operational?

What "healthy" looks like: A recent test restore with the date, result, and owner documented.

Hardware and Infrastructure

Equipment ages quietly, until it doesn't.

Ask:

- What's out of warranty or unsupported?
- What devices aren't patching consistently (and why)?
- Are we replacing proactively—or waiting for failure?

What "healthy" looks like: A simple replacement roadmap and monthly patch reporting.

Access and Credentials

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

Ask:

- Do we have a current user list (including admin accounts)?
- Are former staff/volunteers/vendors fully removed?
- Are shared accounts hiding who did what?

What "healthy" looks like: Quarterly access reviews with a record you can produce.

AI ACCEPTABLE USE

Guardrails, not roadblocks.

AI tools can save time (drafting, summarizing, reporting). But without guardrails, they can also expose sensitive information or create records you didn't intend.

Quick check:
Do staff know what they can and cannot put into AI tools?

A practical AI Acceptable Use policy should cover:

- What data is off-limits (resident/donor info, HR, legal, CJIS-adjacent, etc.)
- Approved tools and who can enable new features
- Required human review (accuracy and public record considerations)
- Safe use cases (drafts, formatting, internal summaries)

RWK can help you create a policy your team can adopt quickly.

CLIENT SPOTLIGHT:

Illinois Municipal Police Department

In 2018, this department was operating on an outdated system prone to breakdowns and data loss, with minimal security protections. They needed a complete modernization with a strong focus on security.

RWK implemented proactive, long-term solutions designed for law enforcement environments, including systems connected to state and federal databases. Since the upgrade, their systems have remained secure – even amid hacking attempts and virus threats – while other organizations have experienced breaches.

"If we had to upgrade our systems again, RWK would be our only choice."
– Illinois Police Chief

...continued on page 4

FREE DOMAIN TRUST SCAN

See how well your domain is protected against email spoofing.

In under 60 seconds, you'll get a score and see whether your email authentication is helping, or leaving you exposed to impersonation.

What you'll see:

- **Your SPF/DKIM/DMARC status (and whether it's enforced)**
- **Spoofing/impersonation risk indicators**
- **A plain-English "what to fix first" summary**

Scan the QR or visit: www.rwksolvesit.com/domain-scan

QUESTION OF THE MONTH

If a spoofed email looked like it came from your CEO/Chief/Director…

Would your team know the first 3 steps, and who owns each one?

FAST CHECK:
Can you disable suspicious access (users & vendors) in 10 minutes?

...continued from page 3

Even well-run organizations accumulate risk over time, especially with turnover, vendors, and urgent work. That's why a checkup matters: it finds the hidden issues before they become an incident.

Most organizations focus on prevention, and that's smart. But resilience comes from knowing what happens next: how you respond, how you document, and how you recover. That's where incident response and AI guardrails belong.

INCIDENT RESPONSE READINESS

Simple. Clear. Practiced.

An incident response plan isn't for "after you get hacked." It's for the moment something feels off, before it becomes downtime.

Ask:

- Do we have a one-page plan with names and phone numbers?
- Can we isolate a device without guessing?
- Do we know when to contact vendors, insurance, legal, or law enforcement?
- Have we done a 20-minute tabletop in the last 12 months?

What "healthy" looks like:
A one-page plan, roles assigned, a short annual tabletop and documented updates.

DEFENSIBLE IT (AUDIT, INCIDENT, AI)

For government and mission-driven organizations, the goal isn't just "secure." It's defensible, meaning you can show controls exist and are maintained.

A checkup helps you produce evidence of:

- Access reviews (users and vendors)
- MFA coverage on critical systems
- Patch cadence with reporting
- Backup test proof
- Incident response roles and steps
- AI acceptable use guardrails (policy and approved tools)

WARNING SIGNS YOU'RE OVERDUE

If any of these sound familiar, it's time:

- "I'm not sure when we last tested a restore."
- "A vendor probably still has access."
- "We don't have a clean list of admin accounts."
- "We've had suspicious emails that looked internal."
- "We'd scramble to explain controls if asked."

These aren't small issues, they're early symptoms.

THE COST OF SKIPPING THE CHECKUP

Skipping prevention doesn't save time, it shifts cost to a crisis:

- Downtime during critical services and operations
- Increased cyber liability exposure
- Documentation scramble during audits/incidents
- Higher risk of impersonation/fraud

Prevention is quiet and manageable. Recovery is loud and expensive.

ALSO THIS MONTH: ZERO-TRUST APPLICATION CONTROL

Most incidents start small: a risky app install, a browser extension, or admin rights that were granted "temporarily."

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

RWK helps: block unapproved apps and reduce admin sprawl without slowing teams down.