www.RWKsolvesIT.com

AUGUST 2025

RWK DIGITAL DISPATCH

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

THE COMPLIANCE BLIND SPOT:

What You’re Missing Could Cost You Thousands

Many small business owners still think compliance only applies to large enterprises. But in 2025, cyber regulations and insurance requirements are tightening—and small businesses are squarely in the spotlight.

Without proper protections in place, a single breach could cost you more than just downtime. You could face regulatory fines, lawsuits, and even denied insurance claims.

Why Cyber Liability Insurance Is a Game-Changer

Cyber liability insurance isn’t just a financial backup plan. It’s an expectation. If you are insured, Insurers now require businesses to prove they’ve taken reasonable precautions to protect themselves-on paper. That means documented policies, employee training, and an incident response plan aren’t just “nice to have” - they’re deal-breakers.

🚨 44% of claims are denied due to missing documentation

⚖️ 20% of ransomware attacks result in lawsuits

💸 Noncompliance can lead to fines ranging from $5,000 to $100,000 per month

Critical Requirements You Need Covered If You Have Cyber Insurance

Cyber Liability Essentials - Documentation

RWK’s Cyber Liability Essentials program helps your organization build and maintain the core documentation insurers and regulators expect:

- An approved Acceptable Use Policy (AUP)
- A secure portal for compliance records
- Evidence of employee security training
- A documented incident response plan
- A data inventory outlining what’s most critical
- One-click reporting for insurance or legal review

Without this paper trail, your cyber insurance claim could be denied—even if you had the right protections in place.

CPAs, Finance, Dealerships Take Note

If your business handles consumer financial data, you must comply with the FTC Safeguards Rule, which includes:

- A written information security plan
- A designated compliance leader
- Ongoing risk assessments

continued on page 2...

...continued from cover

- Multifactor authentication (MFA)
- Oversight of third-party vendors

Violations can lead to **$100,000 fines per incident** for businesses and **$10,000 for responsible individuals.**

ALL Security-Minded Businesses

Insurance and compliance aren't just boxes to check—they require ongoing effort. Proactive organizations:

- Perform regular risk assessments
- Keep policies and training up to date
- Maintain visibility into their security posture
- Engage partners like RWK to guide their efforts

Cyber liability protection isn't a one-and-done initiative—it's a living, breathing part of your business strategy.

Real-World Consequences Of Noncompliance

It's not just theory. One small business experienced a ransomware attack—and because they lacked a documented response plan, their insurance claim was denied. They were left footing the bill, managing legal fallout, and rebuilding trust with clients.

Steps To Ensure Compliance

1 **Conduct Comprehensive Risk Assessments:** Regularly evaluate your systems to identify and address vulnerabilities.

2 **Implement Robust Security Measures:** Use encryption, firewalls and MFA to protect sensitive data.

3 **Train Employees:** Ensure your staff understands compliance requirements and best practices.

4 **Develop An Incident Response Plan:** Prepare for potential breaches with a clear action plan.

5 **Partner With Compliance Experts:** Engage professionals who can guide you through the complexities of regulatory requirements.

Don't Wait Until It's Too Late

Compliance isn't just a legal obligation – it's a critical component of your business's integrity and longevity. Ignoring these requirements can lead to devastating financial penalties and irreparable damage to your reputation.

Don't let a compliance blind spot jeopardize your success.

RWK IT Services at MSPCE – A Successful Session on AI and Data Security

RWK IT Services was proud to exhibit at the Midwest Security & Police Conference and Expo (MSPCE) this August—and the event was a resounding success! Our CEO, Jeff Reiter, took the stage as a featured speaker, delivering a powerful presentation titled "Stop AI from Becoming Your Next Data Breach."
Speaking to an engaged audience of law enforcement and municipal leaders, Jeff explored the rapidly evolving role of artificial intelligence in public sector environments—and the urgent need for proper guardrails. As AI tools become increasingly integrated into daily operations, Jeff emphasized how critical it is to balance innovation with responsible, secure implementation.

His session covered:

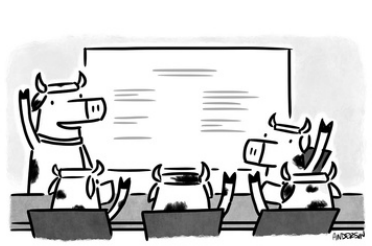
✅ How to create and enforce an acceptable use policy for AI
✅ Key AI security risks and how to avoid them
✅ Real-world examples of AI-related data breaches
✅ Best practices for safe, compliant AI adoption in public safety settings

We had incredible conversations at Booth #601, where RWK's team connected with police departments, municipalities, and public safety officials seeking practical, proactive IT solutions.

Want to dive deeper into AI safety for your department?

We now offer AI awareness training for public agencies. Learn more or schedule your session: www.RWKsolvesIT.com/ai-presentation

CARTOON OF THE MONTH



"Another unanimous vote! Man I love the herd mentality!"

JESSE COLE

ON HOW TO CREATE RAVING FANS

Jesse Cole built the iconic Savannah Bananas brand from nothing by doing things differently. The key to his success was his "fans first" mindset, which centers on creating an incredible experience for each individual fan.

"[Fans] aren't buying because of the product," Cole explained. "They're buying it because of how we make them feel. That's the differentiator."

Here are his takeaways for businesses who want to create raving fans too.

Eliminate Friction.

Put yourself in the customer's shoes and eliminate the friction they experience. Just like Walt Disney used to walk around Disneyland every day to find things to improve, businesses should go through the sales and onboarding process to look for friction points—and reduce them whenever possible.

Entertain Always.

The heart of entertainment is to provide enjoyment, according to Cole. "How do you map the journey for your customers, every step of the way, to provide enjoyment and make their lives better?" he said. Think about the little details; there are many stages of the experience of working with you, from first impressions to onboarding. Try to make every stage remarkable. Those interactions set the tone when someone starts working with you.

Experiment Constantly.

And don't just experiment—try the exact opposite of what's normal. Not every experiment will work, but the ones that do have the opportunity to become groundbreaking successes. And people only remember the successes, not all the failures along the way.

Engage Deeply.

"Do for one, what you wish you could do for many," Cole said. The Magic Castle Hotel in Hollywood is a master of this tactic as well; their CEO says the key is to "listen carefully, respond creatively." By creating tailored experiences for individuals, you show your entire fan base that you care deeply for the people who support you.

Empower Action.

"Stop standing still, start standing up," said Cole. "None of [the rest of it] matters if we don't empower first ourselves, and then our team." To this end, he advised businesses to not underestimate the power of a thank you—to your team, your mentors and your clients—when it comes to building raving fans.

SHINY NEW GADGET OF THE MONTH

Withings Omnia Smart Mirror

The Withings Omnia Smart Mirror is a concept health device that centralizes wellness tracking at home. It performs daily 360° health scans, measuring heart metrics (ECG, AFib, vascular age), body composition, sleep quality, activity, and nutrition. Integrated with the Withings ecosystem, it delivers personalized insights via an AI voice assistant and allows users to share data with clinicians through the Withings+ app. Features like 24-hour cardiologist reviews are included via Cardio Check-Up. Though not yet available for purchase, select features will launch in the Withings app later this year. Omnia was unveiled at CES 2025.

Unlocking the Power of AI in Local Government

At this year's TOI Q&A Days in June, our CEO Jeff Reiter delivered a timely and eye-opening presentation on how AI tools like ChatGPT and Microsoft Copilot are transforming Township operations.

From drafting reports in seconds to simplifying budget planning and legal research, Jeff showed attendees how AI can be a powerful assistant – not a replacement.

He also issued a critical reminder: with great tech comes great responsibility. Townships must have clear policies to ensure sensitive data stays protected while reaping AI's productivity benefits.

Jeff's talk, "An Introduction To Artificial Intelligence" is perfect for company trainings, association events, and leadership meetings. Want to bring this talk to your group?

YOUR PHONE CAN BE TRACKED

And It's Easier Than You Think

Most of us carry our phones everywhere, trusting them with everything from passwords to private business conversations. But here's the sad truth: phone tracking is far more common – and easier – than most people realize.

Whether it's a jealous partner, a disgruntled employee or a cybercriminal targeting your business, anyone with the right tools can monitor your location, read your messages or even access sensitive business data without you ever knowing. And for business professionals, that puts more than just your privacy at risk. It puts your operations, clients and bottom line in danger.

How Phone Tracking Works:

There are several ways someone might track your phone:

Spyware Apps: These can be installed to monitor calls, texts and app usage. Some can even activate your microphone or camera without your knowledge.

Phishing Links: Clicking a malicious link in an e-mail or SMS can silently download tracking software onto your phone.

Location Sharing: Apps with excessive permissions or with social platforms you forgot were still logged in might be sharing your location in the background.

Stalkerware: This spyware is designed to hide in plain sight, often disguised as harmless apps or settings tools.

These methods don't require advanced hacking skills – many are sold commercially under the guise of "monitoring software".

Why This A Big Deal For Business Professionals

If you run a company, your phone likely contains more than just personal messages. Think: e-mails with confidential client data, saved passwords, banking access and employee records. A compromised phone can be an open door to your entire business.

The scarier part is the likelihood that you won't realize you're being tracked until it's too late, after an account is drained, a deal is leaked or customer trust is broken.

Consider this: a single data breach costs US small businesses an average of $120,000 (Verizon Data Breach Investigations Report). If your device is the weak link, that breach could start in your pocket any time.

Signs Someone Might Be Tracking Your Phone

Most spyware tools are designed to operate quietly, but there are still signs to watch for:

- Battery drain that doesn't match usage
- Increased data usage or strange spikes
- The phone feels hot when idle
- Unexplained apps or icons
- Background noise during calls
- Frequent crashes/unresponsive screens

These symptoms don't guarantee your phone is compromised, but when paired alongside other unusual behavior, they're worth investigating.

How To Stop Phone Tracking

If you suspect someone is tracking your phone, here's what to do:

1. Check App Permissions: Go through your app list and review permissions. Disable unnecessary access to location, microphone and camera – especially for apps you rarely use.

2. Update Your Phone: Security updates often include patches for vulnerabilities that spyware might exploit. Make sure your phone is running the latest OS, always.

3. Perform A Factory Reset: If spyware is confirmed and can't be removed easily, a factory reset is the most thorough option. Just make sure to back up critical data, complete the reset and then change all important passwords.

4. Set Up Security Controls: Use biometric logins (like Face ID or fingerprint) and enable multi-factor authentication on business apps.

Don't Leave Your Phone – And Business – Exposed

Because you're a business professional, your phone is more than a personal device. It's a mobile command center, customer file cabinet and sometimes a virtual vault. That's why keeping it secure should be a priority.

Cybercriminals are opportunists, and a compromised mobile device gives them an easy way in – no firewall needed.