

The 2025

IT SERVICES BUYER'S GUIDE

For the Greater Chicago Area

You've got a business plan.

Do you have an IT roadmap?

IT SERVICES BUYER'S GUIDE

- 04 Chapter 1** – The 5 big technology revolutions affecting Greater Ch. organizations like yours
- 08 Chapter 2** – You’ve got a business plan—do you have an IT roadmap?
- 12 Chapter 3** – Why leaders switch IT partners (and how to spot the signs)
- 20 Chapter 4** – Safeguard what matters most in your organization
- 24 Chapter 5** – Why healthy skepticism of IT providers is smart
- 30 Chapter 6** – What every IT firm wishes you already knew about tech
- 36 Chapter 7** – Helping your in-house IT: how we team up
- 40 Chapter 8** – Don’t just take our word for it: Chicagoland client stories
- 44 Chapter 9** – About us
- 46 Chapter 10** – Your first 90 days: what to expect
- 50 Chapter 11** – Ready to move? What to do next

CHAPTER 1

The 5 big technology revolutions
affecting Greater Chicago
organizations like yours



Hello, my name's Wylie Blanchard Jr and I'm the owner of Reintivity Technology Solutions



Wow... It's been a wild stretch for leaders like us.

Whether you're growing steadily or hustling for every new client, you've felt how fast business tech has shifted under our feet..

We're living through a cluster of massive, connected tech shifts.

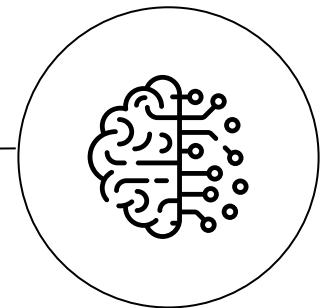
Five, in particular, are reshaping the day-to-day for the organizations we support. I believe we're in the middle of a series of massive and interrelated technological revolutions.

Revolution 1) AI

Go back to late 2022 and most people still filed "AI" under science fiction—something for "someday."

Then tools like ChatGPT hit the mainstream, and the AI wave broke. Since then, assistants like Microsoft Copilot and Google Gemini have popped up inside everyday apps. Even if you've never opened them, AI is already embedded in workflows: triaging patient messages, pre-drafting board updates, summarizing case notes, or spotting anomalies in claims.

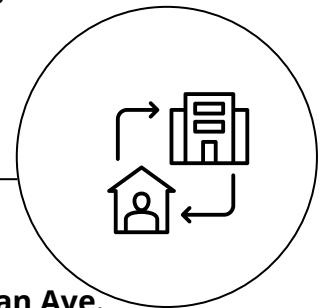
It's only the opening act of this revolution, and the pace is accelerating.



Revolution 2) Hybrid working

Lockdowns didn't invent flexibility—they fast-forwarded it. Today, your people expect work that travels: home, office, a campus library, a field office, or that quiet coffee shop off Michigan Ave.

The challenge is to make "work from anywhere" secure, collaborative, and productive. Teachers need to meet students online without friction. Caseworkers must update records on the go. Adjusters and program staff should serve clients without roadblocks. The tools enabling this evolve constantly; it's worth revisiting how your organization communicates and collaborates.

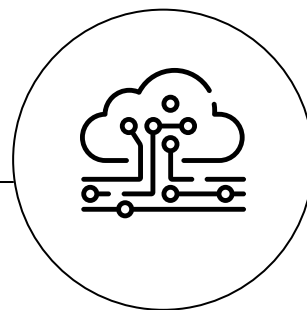


Revolution 3) Cloud computing

“Anytime, anywhere, any device” works because your apps and data live in the cloud. Remember when reporting meant being physically in the office? Feels ancient now.

That freedom is incredible—but it also means data is moving more places than ever. Governance, identity, and protection matter more with each new SaaS login, file share, and integration.

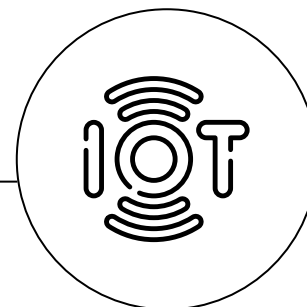
The cloud liberates us—and demands discipline.



Revolution 4) Internet of Things (IoT)

If a refrigerator can go online, everything will. Exam-room tablets, classroom devices, door controllers at municipal buildings, sensors in community centers—IoT is everywhere, offering convenience and insight.

But every device that talks to your network expands the attack surface. Without clear standards for what's allowed on your environment—and how it's segmented and monitored—you're inviting risk you can't see.



Revolution 5) The biggest security risk we've ever seen

Big change attracts good actors and bad ones. Cybercriminals now run industrial-scale operations that target organizations of every size, all the time.

It really can take just one convincing phishing email to grant access to your entire environment.

Attackers often hide for weeks before striking. If you saw what we see daily, you'd understand why we weave security into every other revolution—it's not an add-on, it's the foundation.



Threats grow in volume and sophistication yearly. That doesn't call for panic; it calls for calm, layered defenses and clear training.

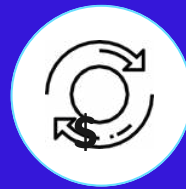
People remain your first line, so your tools must support them—reducing friction while raising protection.

We stay on top of best-practice controls and continuously evaluate new security tools to keep clients safe. We're happy to walk you through what's essential and what's just buzz.

Here's the technology strategy we recommend and implement:



Defend: Protect identity, endpoints, email, and data with MFA/SSO, patching, device management, backups, and 24/7 monitoring/response. Add real-world security awareness training so your team recognizes risks without slowing down the mission



Invest: Make technology propel your work, not hinder it. Standardize, automate, and integrate. Re-evaluate collaboration, cloud apps, voice, and analytics so care teams, educators, adjusters, program staff, and clerks spend more time on impact and less on workarounds.

If you're reading this, there's a good chance you're not 100% thrilled with your current IT support and you're exploring a change.

Of course, we'd love to earn your trust.

This guide shows you how a true IT partner behaves, what great support looks like, and why data security and IT strategy belong at the core of your long-term plans.

If you're ready to talk sooner, flip to Chapter 11 to schedule a conversation. Let's see how we can partner to help your organization thrive this year.



Wylie Blanchard Jr
Founder - Reintivity Solutions
312.985.6810
info@reintivity.com



CHAPTER 2

You've got a business plan—
do you have an IT roadmap?



When's the last time you refreshed your IT strategy?

If your answer is “what IT strategy?” or “not lately,” this is your sign.

Whether your tech footprint is a single point-of-sale, a handful of laptops, or a multi-site network with phones, apps, and cloud tools, a real strategy is your best ally. It's the difference between treading water during uncertainty and surfing the wave.

Yes, I'm biased—but only because we see the outcomes daily. A thoughtful IT strategy is a core ingredient in every successful organization we support.

Your strategy should sit right next to your business plan. It translates goals—patient access, student success, faster claims, better resident services, mission impact—into the technology moves that get you there. It should include near-term wins and long-term bets, and it should leave room to pivot when things change (because they will).

And while it's called an “IT strategy,” it's not actually about the gadgets. Sure, you'll choose platforms and devices, and map migrations you'll tackle later. But the real point is your organization—how technology clears roadblocks, amplifies people, and makes the important work easier.

A practical place to begin: inventory today's setup. What hums along? What frustrates people? As you grow—adding clinics, classrooms, caseworkers, or programs—will your tools keep up, or will you need new systems, integrations, or voice solutions to scale? Talk to your team. Ask what helps and what slows them down. Where are the extra clicks? What tasks feel duplicative? Could secure single sign-on save time? Would two systems talking to each other eliminate manual rekeying? Reality on the ground is the best data you'll collect.

When you partner with a proactive IT firm, they'll help you choose the right hardware and software for how you actually work (and how you want to work). They'll spot risks you haven't noticed and suggest simpler ways to deliver care, teach, process claims, serve constituents, or manage programs.

A living technology roadmap is the keystone of that strategy. It gives you clarity on timing and spend—what's coming next quarter versus next year—so upgrades and renewals don't ambush your budget. No surprise invoices. No mystery emergencies. Just planned progress.

Could you build this alone? Maybe. But a proactive partner will co-create it with you and keep it current as your environment and priorities evolve.

Make every dollar pull its weight

Budgets are under a brighter spotlight than ever.

Every expense should pull measurable weight for your mission. Create simple metrics that show whether your stack is earning its keep: uptime, ticket trends, adoption, time saved, compliance posture, risk reduction, user satisfaction, even outcomes like visit throughput or student engagement.

People may *like* a tool's interface, but if it's not moving the needle, it's not doing its job. Measure what matters, then adjust.

Your IT partner should schedule regular strategic reviews—twice a year works well.

Celebrate what landed, unpack what slipped, realign to current goals, and refresh the roadmap. That cadence keeps the plan useful instead of “shelfware.”

Why we say “partner,” not “provider”

Picture an office building.

One role is the evening cleaner—they show up after hours and tidy the mess.

That's how many IT shops operate: they fix what's broken.

We prefer the facilities manager model.

This person plans maintenance, schedules upgrades, and prevents problems before they start. They still supervise the cleaning, but most issues never become emergencies.

That's what a proactive **IT support partner** does. We harden identity, patch devices, monitor signals, test backups, and tune configurations quietly in the background so fewer things break in the foreground.

Of course, some incidents still happen—technology moves fast, and so do attackers.

When it does break, we fix it.

But the point of the strategy is that you're recovering from fewer fires, with smaller impact, and faster.



For clients across Chicagoland—clinics, schools, insurers, agencies, and non-profits—we maintain an ongoing, rolling roadmap. Together, we know exactly:

- **What's planned in the next 24–36 months** (cloud moves, device refreshes, app retirements, security milestones).
- **What investments are coming and when** (so finance and leadership aren't blindsided).
- **Which items are movable** (to pause during tight months or pull forward when funding arrives).

That visibility means no surprises. Strategic reviews keep both of us aimed in the right direction, even as regulations shift, grants cycle, or programs expand.

This only works because it's a partnership. We learn your rhythms—busy seasons, reporting deadlines, accreditation dates—and we treat your environment like it's ours. That context lets us recommend the right “now,” “next,” and “later,” and it keeps technology aligned to outcomes, not just features.

In short: a documented strategy plus a living roadmap equals fewer headaches, smarter spend, and a team free to focus on impact instead of workarounds. That's the point—whether you're delivering care, educating students, paying claims, serving residents, or advancing a mission that matters.

CHAPTER 3

Why leaders switch IT partners (and how to spot the signs)



If you're reading this, there's a decent chance your current IT relationship isn't delivering.

We hear from plenty of Chicagoland organizations who feel stuck—service is slow, security feels fuzzy, and strategy is nowhere to be found.

Below are the most common reasons teams decide it's time for a new **IT support partner** (not just a provider).



REASON TO SWITCH 1) YOU'RE NOT SEEING BUSINESS RESULTS

Return on investment rules the day—especially now.

You should be able to glance at a simple report and know exactly how hard your IT partner has worked and what that effort delivered for your organization:

- fewer disruptions,
- stronger security,
- smoother workflows, and
- real movement on goals

like patient access, student engagement, accurate claims, better resident services, or mission impact.

A true **IT support** partner brings a clear near-term and long-term strategy—and backs it with meaningful metrics you can trust. Those measures must be tailored to your world, not a generic bundle padded with jargon.

If the numbers are vague or hard to decipher, they're not helping you steer the business. In short: relevant metrics + a living strategy = visible results. If you don't have that, it's time to consider a switch.



REASON TO SWITCH 2) COMMUNICATION IS SLOW OR SLIPPERY

This covers a whole spectrum—from slow acknowledgements and vague status updates to missed callbacks when you were promised one. With any other supplier those gripes might seem minor, but when technology underpins patient care, classrooms, claims, resident services, and fundraising, “small” comms issues balloon into big operational risks.

It’s also a classic way to tell the difference between an IT provider and an IT partner. A partner is responsive and predictable, not slippery or silent.

Again, this is another way for you to distinguish an IT support provider from an IT support partner.

You need a partner who:

- Acknowledges issues promptly, so you know it’s in motion,
- Keeps you in the loop on what matters—no surprises, just clear next steps,
- Does what they say they’ll do, when they say they’ll do it.

Because your wins are their wins—and your setbacks are theirs too—the faster an issue is acknowledged, communicated, and resolved, the better it is for both teams.



REASON TO SWITCH 3) SECURITY ISN’T TREATED LIKE THE FOUNDATION

Yes, it happens.

Some support firms—tasked with protecting your data—don’t hold themselves to the same standard. They skip ongoing learning about new scams and threats, which means they can’t fully protect you.

They also won't go the extra mile to lock down every corner of your environment or keep software reliably up to date.

That should worry any organization handling sensitive records—patients, students, policyholders, residents, or donors.

Ask yourself: is this really who you want defending your organization as attacks and breaches keep rising?



REASON TO SWITCH 4) “NOT IN THE CONTRACT” BECOMES A CATCH-ALL

“Sorry, that’s not covered.”

If you’ve heard that from your current IT shop, take it as a warning—when the request is clearly about your technology, that response signals the wrong mindset.

“We don’t cover that” usually means they’re more focused on protecting their scope than protecting your organization. That’s not how a partner behaves. A true IT support partner looks for ways to strengthen your network, tighten data security, and improve infrastructure—not just tick off items in a rigid, one-size-fits-all agreement.

You deserve a partner who adopts your goals as their own and does as much as possible to help you reach them—whether that’s safer patient access, smoother classroom tech, cleaner claims, more responsive city services, or stronger nonprofit programs



REASON TO SWITCH 5) FIXES TAKE FOREVER—AND SILENCE FILLS THE GAPS

Not every problem can be patched in an instant. Tricky issues sometimes need extra diagnostics; rare glitches may take real sleuthing.

That's normal. What isn't normal is the blackout between "we're looking into it" and "it's solved." In those longer investigations, **communication is everything**. If your partner is updating you at each step—what they tried, what's next, when to expect news—you can trust the fix is moving.

But when a ticket sits untouched for days, you've got a different problem. Three days without a response isn't a queue; it's a warning sign. Worse, some issues never truly get resolved—or a "fix" quietly breaks something else down the line. That's not bad luck; that's a support process that needs an overhaul.

Technology will misbehave. We all know that. Still, you shouldn't be stuck in a cycle of recurring issues, long waits, and radio silence—especially when your team is caring for patients, teaching students, processing claims, serving residents, or running programs. Every extra hour of waiting is downtime for your organization... and where's the value in that?

A responsive **IT support partner** keeps you informed, contains impact, and closes the loop—fast. If that's not your current experience, it may be time to switch.



REASON TO SWITCH 6) NOBODY OWNS THE PROBLEM

An IT relationship only works when both sides own their part—and a good partner owns theirs without hedging.

When accountability goes missing, trust evaporates and the partnership stalls. If your provider dodges responsibility when something breaks, that's your sign the relationship is headed nowhere useful.

We hear the same two red flags again and again. First: you report a problem and get told it's your fault—even when you followed their instructions to the letter. Second: you're bounced to "call the software vendor" or "take it up with someone else," as if vendor-wrangling isn't part of the support you're paying for. Neither response reflects partnership; both are buck-passing.

A true **IT support partner** quarterbacks the fix.

They take point in their domain, coordinate with third parties when needed, and keep you focused on your real work—care, classrooms, claims, resident services, or mission delivery. If they're handing the problem back to you instead of stepping in, you're not getting the benefit of a partner at all. Time to upgrade.



REASON TO SWITCH 7) TECH TALK INSTEAD OF PLAIN ENGLISH

If technology were simple, every team could run its own infrastructure without help.

But it isn't. It's packed with unfamiliar terms and shifting concepts—and some days it feels like everything changes every 7 minutes. For non-specialists, that maze can be overwhelming.

A good **IT support partner** does the opposite of confusing you: they turn complexity into clarity. They make hard things look—and sound—easy, explaining options and trade-offs in plain English, not a foreign language.

This matters most in real life: a principal weighing classroom tools, a clinic manager approving a security change, an insurance ops lead greenlighting a workflow tweak, or a nonprofit ED reviewing a grant-funded upgrade. If you can't communicate clearly as partners, the relationship stalls, frustration grows on both sides, and your organization can't fully benefit from the technology you already own.

Bottom line: if conversations leave you more confused than confident, that's a sign to switch to a partner who translates tech into decisions you can actually use.



REASON TO SWITCH 8) YOU'RE NOT LEARNING ANYTHING USEFUL

No one expects you to become an engineer—that's why you hire a partner. But a good IT support partner should help you learn just enough to stay safe and confident.

You should pick up practical basics over time: how modern scams work, which signs to watch for, and simple ways to protect sensitive records across clinics, classrooms, claims, and community programs.

If the message you hear is "Don't worry about it—we'll handle everything," that's a red flag. You can't protect your organization if you don't understand what you're defending against, even at a high level.

Great partners also narrate their work. They explain what's being changed and why, so you gain a plain-English grasp of how your setup works. That context helps your team troubleshoot small stuff quickly—and know exactly when to call for help.



REASON TO SWITCH 9) THE ANSWER ALWAYS SEEMS TO BE "BUY MORE HARDWARE"

We hear this a lot: the previous IT team seemed more excited about selling shiny devices than strengthening the basics.

gear can be great—but it's rarely the first priority. Before anyone recommends laptops, tablets, phones, or switches, your partner should focus on fundamentals that move the needle: identity, backups, patching, email security, device management, and network hygiene.

Yes, you need a certain level of equipment to operate smoothly. But most Chicago-area SMBs in healthcare, education, insurance, government, and non-profit already own enough to work effectively. For many organizations, getting the **infrastructure** right beats buying more gadgets. Extra devices are often "nice to have," not mission-critical.

A proactive **IT support partner** will help you build a living IT roadmap that schedules refreshes on purpose. You'll know which upgrades matter, why they matter, and when to budget for them—so spending tracks value and you avoid surprise purchases.



REASON TO SWITCH 10) YOU'VE OUTGROWN THEM (AND THAT'S OKAY)

This one isn't "bad"—it's a sign of progress. Sometimes your organization simply becomes too complex for a smaller IT shop to handle well.

That's a win for your growth, but the tricky part is knowing when to make a change, especially if you genuinely like your current team.

Keep an eye out for these tells:

- responses slow down just when you need faster turnaround;
- fresh, strategic recommendations dry up;
- or you require a higher level of support than they can realistically provide.

If any of that rings true, it's in your best interest to find a new **IT support partner**.

If you're feeling the strain and need more from IT, chances are your current partner sees it too. The good ones will raise the topic before you do. No drama—no team wants to operate beyond its depth or hold you back.

If any of the pain points we've covered sound familiar, this might be your moment to change partners.

When technology sits at the core of your growth plan, the value of a trusted partner becomes obvious.

We're not perfect—no firm is. Humans build and run these systems, and sometimes we miss.

What matters is the relationship. Because we work as true partners with our clients, we can have direct, grown-up conversations and pivot fast. Instead of patching over bruised feelings, we set clear expectations, make the right adjustments, and get issues resolved quickly.

CHAPTER 4

Safeguard what matters
most in your organization



As the last few years proved, being able to work from anywhere, at any time, on any device feels empowering.

Flexible work pays real dividends: lower overhead, wider candidate pools, and teams that are happier and more productive—whether they're in a clinic, a classroom, a field office, or on a site visit in Bronzeville.

But as phones, tablets, and laptops keep getting smarter, they've also become... disposable. Most of us can run our day from a handset now. And let's be honest—devices get dropped, misplaced, or cracked more often than we'd like to admit.

The good news? Because your files live in the cloud (think resilient, geo-distributed servers), a lost phone isn't a meltdown. You pick up a new device, sign in, restore from backup, and—presto—your apps and data reappear. The same “easy button” applies to tablets and laptops. These days, a lost device is mostly an inconvenience and a modest expense.

That flexibility is fantastic—but it introduces risk. The moment a device leaves the office, your data can be exposed. Bad actors work around the clock to pry it open, copy it, or lock it away from you.

You've likely heard of **malware**. Short for malicious software, it's code that sneaks onto a device or network to spy, steal, or sabotage. Once it's in, it behaves exactly how the attacker designed—often quietly—and can be stubborn to detect or remove.

Even scarier is **ransomware**, the fastest-growing cybercrime. If you're not taking the right precautions, odds are you'll encounter it sooner or later. Ransomware encrypts your data so you can't access it, then demands payment to unlock it—usually in cryptocurrency, often on a ticking clock. Miss the first deadline, the price doubles; wait a week, and you may never see your data again. It's as brutal as it sounds.

And while anyone can be hit, small and midsize organizations are prime targets. Criminals know many SMBs don't invest heavily in security, making them easier marks than big enterprises.

How does it get in? Most often through a single click in a convincing email. Today's phishing messages are slick: familiar logos, near-perfect sender addresses, and simple, plausible asks like “confirm your details.” Even careful people get fooled.

Worse, ransomware rarely detonates immediately. Attackers may camp out for 60–100 days—or longer—probing for weaknesses and moving laterally so they control more of your environment when they strike. By the time the lock snaps shut, eviction is painfully hard.

That's why prevention beats cure every time.

You and your IT support partner should watch for early warning signs, such as:

- New or unexpected **administrator** accounts appearing
- Security tools mysteriously **disabled**
- Unknown **software** being installed
- Long-running **remote access** sessions that span days

There are many deeper technical indicators, but spotting these puts you ahead of the curve.

Training matters just as much as tooling. Your people are the first line of defense, so everyone—from front desk to finance—should get regular, role-appropriate cybersecurity awareness. Software alone can't save you; you need **software + humans** working together.\

It's also important to be realistic: **100% protection** isn't possible. Cybercrime evolves constantly, and defenses must keep pace. You can drive risk down to a tiny fraction—but here's the twist—locking everything down too tightly can backfire. If security adds friction at every turn, busy staff will look for shortcuts, skip steps, or prop open the metaphorical door.

That's why we favor **blended security**. Instead of stacking hoops to jump through, we combine complementary tools and services—identity, MFA/SSO, patching, device management, email filtering, backups, and monitoring—so protection feels smooth and mostly invisible. Fewer passwords to juggle, fewer interruptions, stronger defense.

And the blend is never one-size-fits-all. A community clinic, a K-12 school, an insurance brokerage, a city department, and a nonprofit each face different rules, risks, and workflows. We tailor the mix to your environment, balancing usability with security so your team stays safe and gets work done—anywhere in Chicagoland, on any device, without the drama.



You need to be aware of the signs of a hacker in your network. Both you and your IT support partner should look out for:

- Unexpected new administrators appearing on your network
- Software being disabled
- New software being downloaded
- Remote access sessions lasting for days at a time

Of course there are many technical things to look for but that will give you a good start.

A good IT support partner will always recommend everyone in your business has regular cyber security training. After all, your people are your first line of defense from cyber attack. Software alone won't offer a good level of protection, you need software and humans.

It's important to understand this: you can never be 100% protected from malware, ransomware, and other forms of attack. That's impossible, because it's a non-stop game where the criminals are always inventing something new, and the data security world must catch up.

It is possible to be 99.99% protected, but you may be surprised to learn that we don't always agree with going that far.

You see, when you lock down **everything** to make your data security watertight, what you can accidentally do is frustrate and annoy your staff. They'll have lots of extra layers of protection to go through, more steps in an already busy workload and more to remember.

And what that means in the real world is that they'll skip steps, and look for ways to bypass security. Which puts your business at greater risk.

Think of it like a door to an office. If you have seven big locks and a biometric scan just to open it, eventually, people will get frustrated and just prop the door open!

To remove the frustration and hassle, we use what's called "blended security". We combine several products and services, which work together to protect you. It means fewer codes and passwords for your people, and a better level of security for your data.

And the clever part is that every blend will be different, depending on the business it's for. That way we can customize security perfectly for each client, based on their specific requirements.

CHAPTER 5

Why healthy skepticism of IT providers is smart



You don't know what you don't know about IT—and that's perfectly reasonable.

Why should you track every new platform, patch, or security bulletin?

You've got clinics to run, classrooms to support, claims to process, residents to serve, and missions to fund. Your job is your specialty; keeping up with technology is ours.

Think about your own field. You read trade publications, attend conferences, keep certifications current, and compare notes with peers. That's how you stay sharp. No one expects you to repeat that entire cycle for IT on top of everything else.

Would you expect your clients to know as much about your domain as you do? Of course not—that's why they hire you.

Same here.

We live and breathe the fast-moving, deeply technical world of modern IT. We enjoy the pace, obsess over standards, evaluate tools you'll never have to think about, and calibrate them for real organizations—like a health center in Pilsen, a K-12 network in Evanston, an insurance brokerage in Oak Brook, a city department downtown, or a nonprofit on the West Side.

Plenty of folks consider themselves “IT experts” because they're handy with computers. But great managed service partners operate on a different level—methodical processes, enterprise-grade tooling, measurable outcomes, and an obsession with reliability and security.

Here's the uncomfortable truth: IT support is largely unregulated. There's no governing board that says “you're qualified” or “you're not.” No universal license. No minimum operating standard. In practice, almost anyone can print business cards, spin up a website, and call themselves an IT provider.

That's why healthy skepticism is wise.

If you don't ask the right questions, you could hand the keys to your network—and the privacy of your data—to either a reputable, accountable partner... or to a solo operator working nights from a spare bedroom. (Nothing against humble beginnings; everyone starts somewhere.)

If you're a one-person shop with a single workstation, that bedroom warrior might be a cost-effective fit. But if you're running a growing organization with staff, endpoints, cloud apps, compliance requirements, and stakeholders who depend on you, you'll need more than one person and a toolbox. You'll need process, redundancy, coverage, and strategy.

So how do you avoid picking the wrong IT partner?

Start by looking for **solidity**. Because this industry doesn't enforce a baseline, you have to. Do a little due diligence:

- **Verified expertise:** Do they hold current, relevant certifications (Microsoft 365/Azure, security, networking, device management)? Can they explain what those mean in plain English?
- **Real-world experience:** Have they supported environments like yours—PHI, student data, regulated claims, public records, donor CRMs? Ask for sector-specific references in Chicagoland.
- **Documented processes:** How do they handle onboarding, patching, backups, incident response, and vendor management? "We'll figure it out" is not a process.
- **Security posture:** Do they practice what they preach (MFA everywhere, least-privilege access, monitored backups, logging, and continuous training)? If not, they can't protect you.
- **Service transparency:** Can they show service levels, reporting, and a living roadmap—what's planned next quarter vs. next year—so you're never surprised by spend or downtime?
- **Team depth and coverage:** Who answers after hours? Who covers vacations? Is there redundancy so one person's absence doesn't become your outage?

In short: you don't need to become an IT guru—you just need a partner who already is, and who treats your organization like their own. Stay focused on your mission; we'll stay focused on the tech that powers it.

Next, bring the tough questions.

You're not trying to make a prospective IT partner sweat—but you are trying to confirm they can deliver. Hard questions are how you separate polite promises from real performance.

ASK: “How quickly will problems be fixed?”

Yes, timelines vary by severity—but you need specifics.

- **First response:** How quickly do you acknowledge an issue?
- **Hands-on time:** How long until a technician is actually working it?
- **Resolution targets:** What are the SLAs for critical, high, medium, and low issues?

Walk through real scenarios:

- If a clinic can't access the EHR, when will staff be back in charts?
- If a school loses access to its learning platform mid-morning, how fast is the restore?
- If a ransomware event hits an insurance workflow, what's the step-by-step to recovery—and how long until claims resume?

Then dig into **approach**. Do they follow documented playbooks—or wing it? Can they describe the ugliest incident they've handled, what they learned, and how they've prevented repeats since? You're not judging the mishap; you're judging the response—professionalism, judgment, and calm under pressure.

ASK: “Who, specifically, will look after our account.”

It's easy to focus on tools and pricing and forget the humans you'll actually work with. Don't. The people behind the brand will make or break your experience.

How will your prospective partner assign your **account manager**—by sector experience (PHI, student data, claims, public records, fundraising) or just whoever's least busy? Do they consider work style and personality fit? Will you have a consistent point of contact, or a revolving door?

What's the plan when that person is **on vacation or out sick**—is there a named backup who already knows your environment? Who leads strategic reviews and builds your technology roadmap? If something's not right, who can you escalate to—and how quickly do they respond?

This line of questioning helps you learn how the company is organized—and whether their team complements yours.

*ASK: “What do you do **proactively** so my team has fewer interruptions?”*

Downtime is a budget burner.

You’ve seen it: the network blips, staff can’t reach apps, and productivity nose-dives. Even after service returns, there’s a long tail—reboots, re-logins, unfinished conversations, and lost focus. A 15-minute hiccup quietly morphs into 90 minutes of lost work.

So press for prevention:

- Will they run **continuous monitoring**, patching, and health checks to stop little issues from becoming big ones?
- Are **updates and maintenance** scheduled outside business hours—so classrooms, counters, and call centers don’t grind to a halt?
- Do they offer **failover options** (redundant internet, cached content, offline modes) to keep clinics seeing patients, teachers teaching, adjusters processing, and agencies serving residents—even during maintenance?
- How do they **communicate** during incidents—status pages, alerts, clear ETAs—so people aren’t stuck refreshing and guessing?

The right partner is happy to answer all of this in plain English, with examples and metrics. If the answers feel fuzzy, keep looking.

ASK: “Can you walk me through a deeply technical topic—in plain English?”

You’re not trying to earn a networking certification. You’re testing communication. Can they explain a complex process (say, zero-trust access or immutable backups) without drowning you in acronyms? Do they welcome follow-ups, or get prickly when you probe?

Watch for red flags like “don’t worry about it” or “you don’t need to know that.” In a real partnership, clarity matters: leaders need enough understanding to make good decisions. A great IT support partner educates as they go, translating tech into decisions, trade-offs, and next steps your team can act on.

ASK: “How will you keep up with all the changes in our organization?”

Healthy organizations evolve—new hires, new programs, new locations, new apps, new regulations. Twelve months can transform how you operate.

So ask your prospective IT partner how they'll handle that pace. What do they need to know when staffing shifts, a clinic adds a service line, a school rolls out a new LMS, an insurer adopts a claims tool, or a department launches a resident portal? Will those changes automatically update your support plan, security controls, and licenses—or will you be stuck playing telephone?

You're not shopping for a vendor—you're choosing a partner. That means they should proactively recommend better software, cleaner network designs, right-sized voice solutions, and security that fits how your team actually works.

If they can't track your headcount, workflows, or compliance needs (HIPAA, FERPA, PCI, public records, donor privacy), how can they help you scale, improve, and stay safe?

Look for a team that stays plugged into your world with:

- Regular check-ins (monthly/quarterly) to review goals, risks, and roadmap updates
- A simple change intake process for new hires, terminations, role changes, and device moves
- Clear license and asset lifecycle management so you're never overpaying or under-protected
- Ongoing security posture reviews that adjust controls as your environment shifts

There are plenty of other smart questions to ask, but this one reveals a lot about whether a partner will grow with you—or make you drag them along.

CHAPTER 6

What every IT firm wishes
you already knew about tech



Before you zone out and skip this chapter, quick promise: no alphabet soup, no dense tech-speak. Breathe easy.

What follows are a few simple truths that—if every client knew them—would make everyone’s life easier (yours and ours).

#1: YOUR TECH NEEDS CONTINUOUS CARE. IT’S NEVER “SET IT AND FORGET IT.”



Your devices nag you to update for a reason: things change constantly.

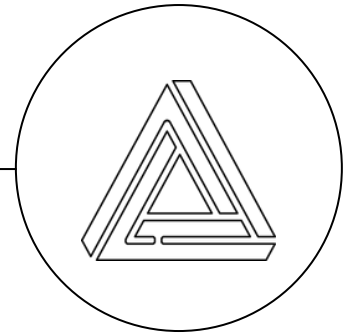
The same goes for your network and core systems. Apps evolve, operating systems shift, hardware ages—nothing stands still. In a clinic, a school, an insurance office, a city department, or a nonprofit, that churn is nonstop.

In professional IT, it’s a given that environments are **monitored and maintained 24/7**. If an offer doesn’t include round-the-clock monitoring and routine maintenance, that’s a hard pass—you’ll feel the pain before the ink dries.

With a solid managed services partner, most of this happens quietly in the background: health checks, patching, alerts, and fixes before anyone at the front desk, help line, classroom, or field office notices a blip.

You won’t see the work—and that’s the goal. Smooth, invisible monitoring and maintenance means your team keeps moving, and “IT drama” never becomes the headline.

#2: THE SUPPORT TRIANGLE (IT'S JUST LIKE THE HARDWARE TRIANGLE)



Here's a handy mental model for buying tech.

Picture a triangle. Its three sides are **quality, speed, and price**.

Stretch one side and the others shift to keep the shape. Choose a faster workstation? You typically pay more, and you're probably buying higher-quality components. IT support follows the same geometry: **quality-speed-price**.

If you go rock-bottom on price, expect trade-offs—slower responses and thinner quality. Invest more, and you usually get faster turnaround, deeper expertise, and sturdier outcomes.

The sweet spot? Decide what you can responsibly invest and aim near the top of that range. Treat support like an **investment**, not a commodity. When your environment and IT strategy are dialed in, hitting business goals—shorter charting time, smoother classroom tech, cleaner claims, better resident services, stronger fundraising—gets a whole lot easier.

#3: BEWARE THE "BEDROOM WARRIOR"



Let's revisit the solo-operator scenario.

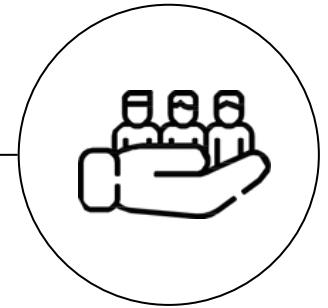
Imagine one person handling your entire support from a spare room. With minimal overhead, pricing looks great.

But remember the triangle—low **price** often squeezes speed and quality. Solo operators rarely have access to enterprise-grade tools, mature processes, or round-the-clock coverage. Those cost real money.

Could it work? Maybe—if **you're their only client** and your needs are tiny. The problem arrives when they add a second client... then a fifth... then more to make ends meet. Response times slip. Proactive maintenance gets skipped. Monitoring falls behind. Not from bad intent—from simple math: one person can't sustainably service many environments well.

Yes, a firm with a **team**, established **processes**, and professional **tooling** costs more. But you're paying for consistent service levels, built-in redundancy (vacations don't become outages), and the capacity to grow without sacrificing quality—whether you're a clinic, a school, an insurer, a city department, or a nonprofit serving Chicago communities.

#4: WE ASK FOR A LONG-TERM PARTNERSHIP—TO PROTECT YOU, NOT US



We don't do hit-and-run IT.

No ad-hoc rescue jobs. No one-off fire drills. We partner for the long haul.

Why?

Sure, recurring relationships are a solid business model—we won't pretend otherwise.

But the *real* win is what a long relationship lets us invest in you.

When we know your organization inside and out, we can:

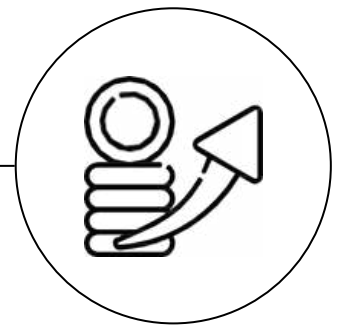
- **Work shoulder-to-shoulder** with your team
- **Understand priorities** and actively help you reach them
- **Design your stack for the future**—IT strategy and infrastructure aligned to where you're going, not where you started
- **Scale with you** as locations, services, and staff grow
- **Strengthen protection** through honest, strategic guidance built on trust

Short-term gigs can't deliver that.

There's no time to learn rhythms, map risks, or tune workflows for clinics, classrooms, claims, city services, or nonprofit programs.

A long-term partnership means shared stakes: when your mission thrives, we thrive. We're not just fixing what broke—we're building, guiding, and safeguarding the technology foundation that helps your organization serve Chicago better, year after year.

#5: WHY OUTSOURCING BEATS HIRING FOR MOST SMBs—MORE VALUE, MORE EXPERTS



When you evaluate IT support, it's natural to wonder, "Should we just hire someone in-house?"

Here's the catch: that single employee ends up wearing every hat—help desk, cloud admin, security analyst, network engineer, trainer, vendor wrangler—and supporting a whole organization at once.

That's a superhero job description, and even superheroes burn out. Shortcuts creep in, not from laziness, but from the laws of time and attention.

With an outsourced partner, your budget buys a **team**: multiple specialists who cover identity, devices, networks, security, backups, and strategy.

You get depth and redundancy—no single point of failure when someone's out sick or on vacation—and work continues after 5 p.m. when it matters.

Yes, the monthly fee may look similar to a salary line.

But what you actually gain is broader expertise, better tools, after-hours coverage, and a roadmap that scales as you grow—so clinics keep seeing patients, classrooms keep teaching, claims keep moving, departments keep serving residents, and nonprofits keep advancing their missions without the "one-person IT department" stress.



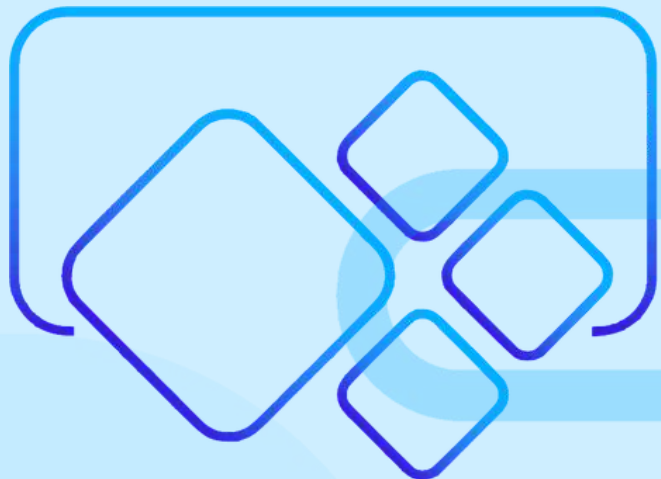
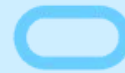
Solve your IT Challenges

Evolve your Business
Technology

with Reintivity Enterprise

Visit:

reintivity.com/enterprise



CHAPTER 7

Helping your in-house IT: how we team up

**Co-managed
IT support**



The background image shows a hand holding a tablet. On the tablet screen, there is a network diagram. A large teal circle on the right contains the text 'Co-managed IT support'. Several smaller circles are connected to this central circle by thin lines. These smaller circles contain icons: three server racks, a person, a laptop, a person, a wireless router, a person, a desktop computer, and a person. The overall theme is IT support and teamwork.

Sometimes our clients already have an internal IT person—or a senior leader who “owns” technology even though IT isn’t their day job.

Not because you’re incapable, but because when something big goes sideways—think ransomware or a wide-scale outage—the accountability lands on your desk.

The good news: there’s a smarter way to share that load.

It’s called co-managed IT.

You keep your in-house talent.

We wrap a team around them—only where and when you need it.



Picture it like a giant donut: your internal IT sits in the middle; our support surrounds them.

- **Bottom layer (daily ops):** We handle the high-volume essentials that bog teams down—help desk coverage, patching and updates, device enrollments, monitoring, and routine changes—so your staff in clinics, classrooms, claims, and departments get faster help.
- **Side support (peer-level assist):** We match skill for skill—advising on tricky tickets, vendor escalations, network tweaks, security tooling, and cloud configs. Your IT lead gets a bench to lean on, not a replacement.
- **Top layer (strategy & governance):** We bring roadmaps, budgeting guidance, compliance alignment (HIPAA/FERPA/PCI/public records), and security architecture that grows with your organization.

Our role is to **complement** your internal team with partnership and a strategic view, so there's always senior thinking on tap—not just firefighting.

This setup gets more out of your internal resources and protects you, the accountable leader, with depth, redundancy, and documented best practices.

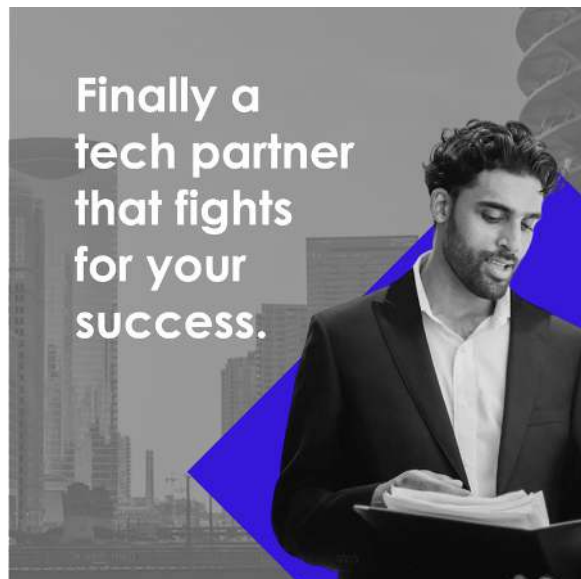
Some IT managers worry an outside partner is a threat.

We're not. We're your amplifier.

Our job is to make you—and your internal team—look great and operate smoothly.

When you succeed, so do we.

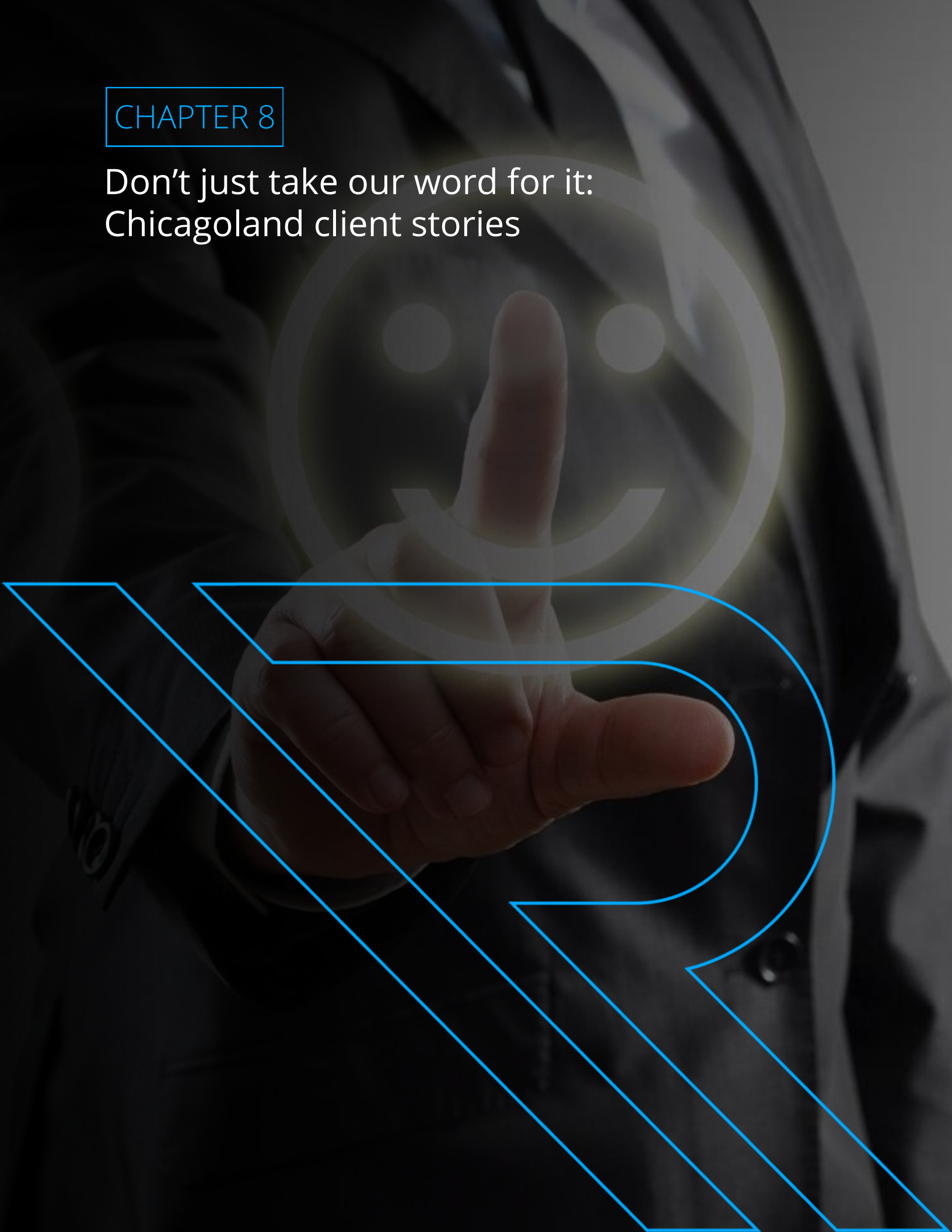
Everyone wins.



Learn more at

CHAPTER 8

Don't just take our word for it:
Chicagoland client stories



We've spent this guide walking through how to choose the right IT support—what to expect, what to avoid, and how to spot real partnership. By now, you know the qualities you want in your own provider.

Of course, that's me—the business owner—making the case for what “great” looks like and how it can transform your organization.

So let's switch seats. Next up, you'll hear directly from Chicago-area clients about what it's actually like to work with us day to day.

Our mission was to reduce major medical episodes and emergency room visits. At a community-based care organization focused on care coordination, we needed a partner who could navigate agencies, privacy rules, and the realities of community work. **Wylie's team delivered—translating Medicaid claims data into practical analyses and daily tasks for our medical director and care coordination teams, enabling family- and community-conscious individualized plans that reduced emergencies and improved overall health.**

Accessible, disciplined, and fair

Louanner Peters,
former Deputy Governor of Illinois;
former Executive Director of an Illinois nonprofit

We brought in Wylie's team for an urgent server failure. **They stabilized it the same day and earned our trust.** We asked them to manage our email, files, and collaboration stack end to end.

The result: predictable systems, clear ownership, and quick responses when we need them.

Robert Jones.
Dialysis Center

What leaders need isn't a more complex tech story—it's clarity and cadence. That's how Wylie works in practice.

Christine Quinn, Ph.D.,
Founder, Living Kindness-Recovery
Community for Families

More client feedback at:
www.reintivity.com

Wylie Blanchard assisted me in creating a vision and developing an incredibly useful digital platform for my business. His company, Reintivity, has consistently **supported my technical needs for the past 10 years**, which has helped my business grow. I found the experience rewarding because Wylie leads with ethics and integrity. I recommend his work for all your IT solution needs.

Maria Malayter, PhD,
Founder, Do What You Love Foundation

I knew when we contacted Wylie that he had always first thought things through as he was consistently both clear and methodical in his presentation. He was always quick to grasp new information and often times ended up **helping me to figure out problems in our state technology systems**. His technical skills seemed very strong. He was always very positive and a pleasure to work with. I always enjoyed interacting with him. I highly recommend the consultant.

Paul Steiber
State Healthcare Department.

Wylie has a talent for looking at extremely complex challenges, designing solutions that are both effective and economical and implementing solutions while ensuring that everyone learns from the process. He is also a pro at uncovering hidden value in others. **Hire his team to do a project, and he is going to deliver several options you never thought were possible.** He exceeds expectations in everything that he does for his clients, his staff and his employer.

Katrina Newton,
Public Health Program.

Wylie's team keeps our cloud productivity environment **stable, secure, and—most importantly—predictable**. That reliability lets us focus on students, not systems.

Dr. Stephen Martin,
Executive Director, CPASS Foundation

Wylie's team has been the partner I wish we'd found sooner: accessible when it counts, responsive without the runaround, knowledgeable across the board, and fair in every conversation.

Andrew Denton,
Founder, Greenbrook Insurance.

Attention Healthcare CEOs, COOs & Directors

STOP LOSING SLEEP OVER IT OUTAGES!

Get the book,

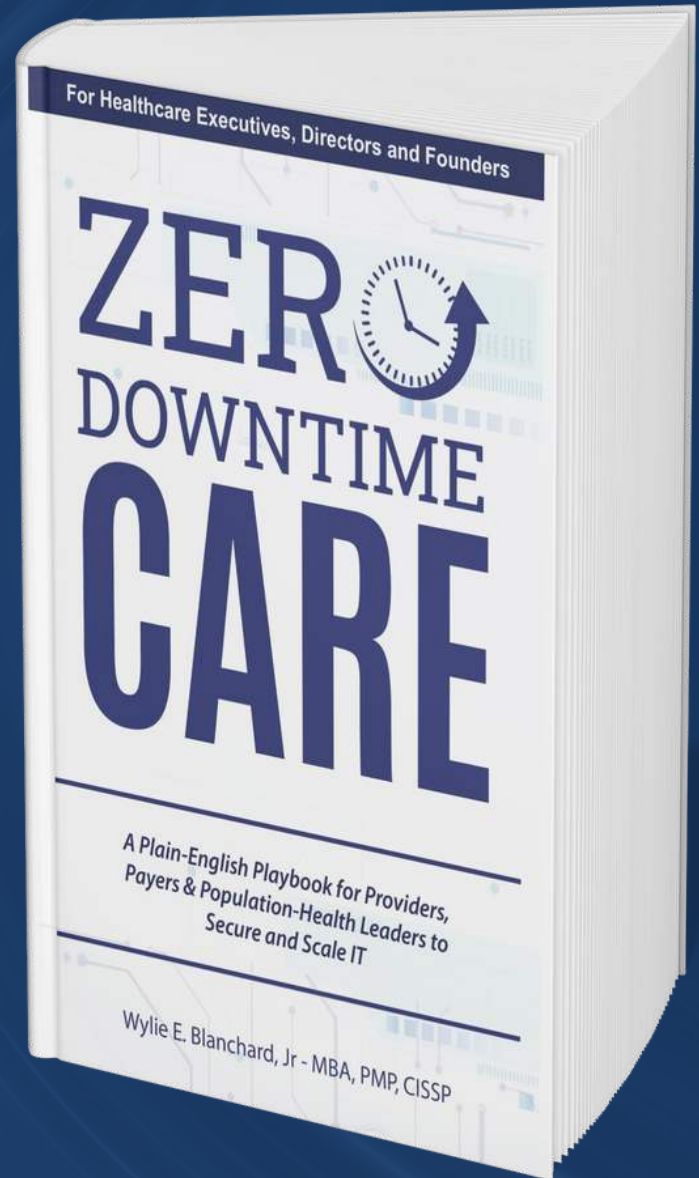
and discover the CARE Modernization™ Framework that lets you secure, scale, and de-risk your entire tech stack—without writing a single line of code.

Get notified of the upcoming book release:
www.zerodowntimecare.com

Stay audit-ready—even while you're deploying brand-new tech.

Every outage and failed audit costs care and cash. This guide gives non-technical healthcare leaders a repeatable roadmap to modernize systems quickly, pass audits, and save seven figures—without writing a line of code.

Learn More at:
www.zerodowntimecare.com



Written by
Wylie E. Blanchard, Jr.
20+ years advising executives and teams on
cloud, cyber-security & compliance.

CHAPTER 9

About us



I love our clients. They always have such wonderful things to say about us.

Let me now properly introduce myself and my business.

A message from Wylie Blanchard, founder at Reintivity Technology Solutions.

My earliest memory of technology is taking apart my family's word processor just to see how it worked—and, to my parents' relief, figuring out how to put it back together. That moment sparked a curiosity and passion that have stayed with me ever since. I've always been fascinated by the challenge of breaking things down, understanding how they work, and creating something better. This mindset has guided me through every step of my journey in the world of technology.

After earning my business degree, acquiring several IT certifications and gaining over two decades of experience across industries like healthcare, insurance and security, I noticed a common thread: businesses were often overwhelmed by the pace of digital transformation. They struggled to integrate new technologies into their operations in a way that made sense for their goals. This insight came into sharp focus after I started Great Tech Pros, the company that would later evolve into Reintivity. I realized that businesses didn't just need IT solutions—they needed a partner who could simplify complexity, provide clarity, and empower them to succeed.

That's why I created Reintivity. Since our humble beginnings in 2013, we've grown from offering database solutions to becoming a comprehensive technology success partner. Today, we specialize in Project Consulting, Managed Services, and Talent Sourcing, providing tailored solutions that help businesses thrive in an ever-changing digital landscape.

What makes Reintivity unique is our focus on people—our clients, our team, and the communities we serve. We don't just deliver IT services; we create partnerships based on trust, collaboration, and results. Whether we're helping a startup scale with cloud solutions or guiding an enterprise through a digital transformation, our mission remains the same: to make technology work for businesses, not the other way around.

Looking back, I can't help but think of that word processor I dismantled as a child. The excitement of figuring out how something works—and the drive to make it better—is what continues to inspire me and our team at Reintivity. Together, we're building smarter, stronger, and more innovative businesses, one solution at a time.

Let's build something amazing together.

— Wylie Blanchard, Founder & Executive Advisor, Reintivity



CHAPTER 10

Your first 90 days: what to expect

If you're curious about partnering with us, here's what to expect from day one.

When we begin to work together, the first 90 days are the most critical.



Our team focuses on three pillars:

1. Learn your organization inside-out
2. Clean up any lingering issues from your previous provider
3. Build a practical, future-ready technology strategy

We're aiming for a long-term partnership, so the first 90 days are all about setting you up to win. You'll get clear expectations—what we do, what we don't, what we'll need from you—and how we can work together like a well-rehearsed crew.

We'll inventory everything: networks, devices, cloud apps, backups, security settings, licensure—the works. The more we know, the better we can protect and optimize. Every finding is documented in our secure system so nothing lives only in someone's head.

We'll also look beyond the “usual suspects.” Website hosting, specialized line-of-business apps (EHR/LMS/claims/permits/CRM), third-party vendors—whether we directly support them or not, we need to understand how they fit together. At some point, you'll have questions about them; we prefer to be ready with answers.

Yes, there's a bit of effort on your side early on—access, introductions, quick interviews—but it's one-time work that pays off for years.

Once we've gathered the facts, we analyze them strategically to understand your environment end to end. Skipping this step isn't “efficient”—it's negligent.

Next, we talk to your people—everyone.

We'll ask what slows them down, what breaks most often, and what they wish "just worked."

We'll also revisit anything your former provider declared "impossible." No promises until we assess it—but count on us to take a fresh look.

Those first 90 days are your reset: stabilize, standardize, and raise the bar so your technology runs at the level your mission demands—and stays there.

Only then do we shift into **forward-looking strategy** together: roadmaps, budgets, modernization, security hardening, and the right upgrades at the right time. The process is tailored to each client—clinic, school, insurer, agency, or nonprofit—so the plan fits your reality, not someone else's template.

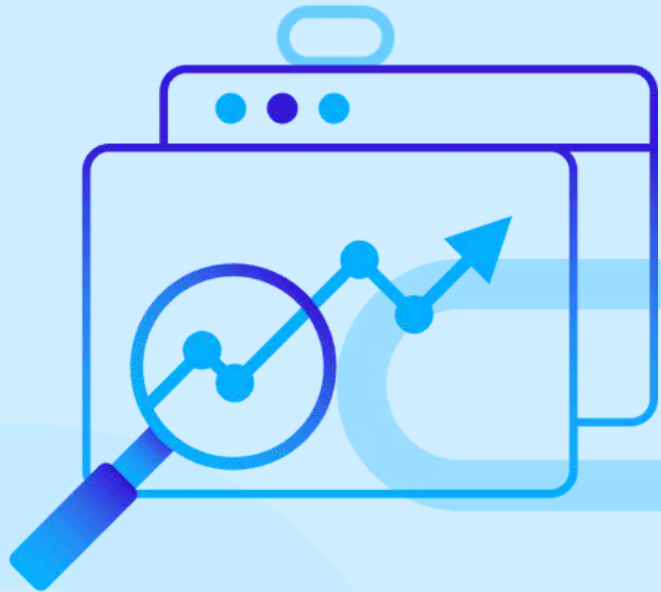
Ready to explore what your first 90 days could look like? Let's connect.



Data & Online Analytics

Get Actionable Insights
from your Data
with Reintivity Enterprise

Visit:
reintivity.com/enterprise



CHAPTER 11

Ready to move?
What to do next



I hope this guide helped answer your big questions about choosing an IT support partner

—and maybe gave you a fresh lens on your current setup.

Good news: we're welcoming new clients right now (that's why I put this together).

love to learn about your organization and goals.

If you're serious about leveling up your technology to support long-term growth, here's the next step:

Book a 15-minute, no-pressure video chat
<https://www.reintivity.com/calendar>

That page shows my live calendar. We'll confirm fit, then schedule a deeper conversation—or an in-person meeting—whichever makes sense.

Of course there's no obligation to buy anything, ever.

No obligation. No hard sell.

I'm looking forward to meeting you and hearing your story.



A handwritten signature in black ink that reads "Wylie".

Wylie Blanchard Jr
Founder - Reintivity Solutions
312.985.6810
info@reintivity.com



This is how you can get in touch with us:

CALL 1.312.985.6810 | EMAIL info@reintivity.com



www.reintivity.com



www.linkedin.com/company/reintivity



www.facebook.com/Reintivity



Serving the Greater Chicago Area