

PLAIN-ENGLISH GUIDE

The Small Business Owner's Guide to Managed IT

Costs, what to expect, and how to evaluate providers. No jargon, no sales pitch.

Indiana & Michigan Edition

Who this guide is for

If you run a small business in Northern Indiana or Southwest Michigan and you are not sure whether managed IT is right for you, this guide is for you. We wrote it for owners and office managers who wear a dozen hats and do not have time to decode acronyms. There is no sales pitch here. The goal is simply to help you make an informed decision, whether you hire us, hire someone else, or decide you are fine as you are.

The short version

Managed IT means paying a flat monthly fee for a provider to proactively run, secure, and support your technology, instead of calling someone only when something breaks. For most businesses with 5 to 75 employees, it costs less than the downtime, security incidents, and lost productivity it prevents. The hard part is not deciding whether you need help. It is picking the right partner.

1

Break-fix vs. managed IT

There are two common ways small businesses get IT support. Understanding the difference is the foundation for everything else.

The break-fix model

You call a technician when something stops working. They bill you by the hour to fix it. It feels cheap because you only pay when you have a problem. The catch: nobody is watching your systems between emergencies, so small issues become big ones, and your costs are unpredictable. Your provider also makes more money when things break, which is a poor incentive.

The managed model

You pay a predictable monthly fee. Your provider monitors your systems around the clock, applies security updates, manages backups, and handles support requests, all included. The incentive flips: a good managed provider makes more money when your technology runs smoothly and quietly, because problems cost them time. Budgeting becomes simple, and security stops being an afterthought.

Dimension	Break-fix	Managed IT
Cost predictability	Unpredictable, billed hourly	Flat monthly fee
Who watches your systems	Nobody, until you call	Monitored 24/7
Security updates	Only when requested	Applied proactively
Provider incentive	Profits when things break	Profits when things run well
Backups	Often unmanaged or untested	Monitored and test-restored
Best fit	Hobby use, 1-2 devices	Any business that depends on IT

2

What managed IT actually includes

Packages vary by provider, but a complete managed IT service for a small business should cover the following. If a quote is missing several of these, ask why.

Help desk and support. A real person to call or email when something is not working, with a committed response time for urgent issues.

24/7 monitoring. Automated tools watch your servers, computers, and network and alert the provider to problems before you notice them.

Patch and update management. Security and software updates are tested and applied on a schedule, not whenever a pop-up reminds someone.

Endpoint protection (EDR). Modern security software on every computer that detects and stops threats, well beyond traditional antivirus.

Managed detection and response. A security team monitors for active threats around the clock and responds when something gets through.

Email security. Filtering for phishing, spam, and malicious attachments, the number-one way attackers get in.

Backup and recovery. Automated, tested backups of your critical data so you can recover from ransomware, hardware failure, or accidental deletion.

Microsoft 365 management. Administration of your email, Teams, SharePoint, and OneDrive, including user setup and security settings.

Security awareness training. Short, regular training so your team can recognize phishing and scams, plus simulated phishing tests.

Onboarding and offboarding. A defined process for setting up new employees and, just as importantly, removing access when someone leaves.

Ask this: If a provider quotes you a low monthly price, ask which of these are included and which are billed separately. The cheapest quote often excludes backup, security monitoring, or training, the three things that matter most.

3

What it costs

Pricing for managed IT is usually quoted per user or per device, per month. The right number for you depends on your size, your security and compliance needs, and how much of your technology you want the provider to own. The ranges below are typical for small businesses in our region as of 2026. Treat them as a planning guide, not a quote.

Service level	Typical monthly range	What you get
Basic managed support	\$75 - \$125 / user / mo	Help desk, monitoring, patching, basic endpoint protection. Good for low-risk offices.
Standard managed IT	\$125 - \$200 / user / mo	Adds managed detection and response, managed backup, email security, M365 management, and security training.
Compliance-grade	\$200 - \$350+ / user / mo	Adds a virtual security officer, formal risk assessments, policy development, and audit-ready documentation for regulated businesses.
Co-managed IT	Custom	You keep internal IT staff; the provider supplies security tooling, escalation, and specialized expertise.

Other costs to plan for

- **Onboarding / setup fee.** A one-time fee, often equal to one to two months of service, to document your environment and deploy tools. This is normal and worth it.
- **Hardware and licensing.** Computers, servers, firewalls, and Microsoft 365 licenses are usually billed separately at cost or a small markup.
- **Projects.** Migrations, office moves, and major upgrades are typically scoped and quoted outside the monthly fee.

How to think about the cost

Compare the monthly fee against the cost of one bad day: a ransomware event that closes you for a week, a wire-fraud email that drains an account, or a server failure with no working backup. Industry data consistently puts the average cost of downtime for a small business in the thousands of dollars per hour. Managed IT is insurance you actually use every day.

4

How to evaluate a provider

Once you decide to explore managed IT, the real work is choosing well. Use these questions in your first conversations. Good providers will answer them directly.

Questions worth asking

What is your guaranteed response time for a critical, business-down issue?

Is cybersecurity included, or is it an upsell? What specifically is covered?

How do you handle backups, and do you test that they actually restore?

Who owns my data, accounts, and documentation if we part ways?

Can you provide references from businesses my size in my industry?

Do you carry cyber liability and errors-and-omissions insurance?

What does onboarding look like, and how long does it take?

How do you keep my team trained against phishing and scams?

Red flags

- **No written response-time commitment.** If they will not put it in the agreement, it is not real.
- **Security is an add-on.** In 2026, security is the core of IT, not an extra.
- **They cannot explain backups in plain English.** Or they have never tested a restore.
- **Long contracts with no exit.** Reasonable terms protect both sides; lock-in protects only them.
- **They badmouth your current setup before understanding it.** Fear-based selling is a tell.

On local vs. national: A regional provider that understands Indiana and Michigan business, can show up in person when it matters, and answers the phone is often a better fit for a small business than a distant national help desk. Ask where their technicians actually sit.

5**If you decide to move forward**

A good engagement follows a predictable path. Knowing the stages helps you set expectations with your team and avoid surprises.

Stage 1: Discovery. The provider learns your business, counts your devices and users, and reviews your current tools and risks. Usually a call plus a short on-site or remote assessment.

Stage 2: Proposal and agreement. You get a written scope of work, pricing, and service commitments. Read the response times, the security inclusions, and the exit terms carefully.

Stage 3: Onboarding. Tools are deployed, your environment is documented, and the top risks are addressed. Expect two to six weeks depending on your size and complexity.

Stage 4: Ongoing service. Monthly support, monitoring, and reporting, with regular business reviews to keep technology aligned with where your business is going.

Want a no-pressure second opinion?

We will review your current setup against this guide and give you a one-page snapshot of your gaps and risks. No obligation, no jargon.

Talk to PTS

hello@phantomts.com
phantomts.com
Serving Indiana & Michigan since 2010

This guide is provided for general informational purposes by Phantom Technology Solutions and does not constitute legal, regulatory, or professional advice. Every organization is different. Use it as a starting point, not a substitute for a tailored assessment. Copyright Phantom Technology Solutions. You may share this document freely in its original, unmodified form.