EDUCATIONAL EBOOK SERIES

The Executive's Guide to Managed IT

How much your business actually needs, what it should cost, and how to choose the right partner.

A foundational guide for Canadian organizations.

hubTGI

hubtgi.com
416-747-1500

INTRODUCTION

Why this guide, and why now

For most Canadian businesses, technology stopped being a back-office function years ago. It is now the floor your whole operation stands on: how your people work, how you serve customers, how you stay compliant, and how you protect everything you have built.

The problem is that IT decisions are usually made under pressure: after an outage, during a growth spurt, when a key person leaves, or at renewal time when a contract lands on your desk. Decisions made under pressure are rarely right-sized. Some organizations pay for more than they need. Far more are quietly carrying risk they cannot see, until it surfaces as downtime, a breach, a failed audit, or a deal lost because a client questioned their security.

This guide takes the pressure out of the decision. It will not tell you to buy anything. It gives you a clear, plain-language way to answer four questions every leader should be able to answer about their own business:

1

What do we actually need?

And how would we know whether our technology fits the business we are today?

2

What should it cost?

What drives the number up or down, and what is a fair price for us specifically?

3

What does good look like?

How do we tell a strong technology partner from a weak one, in practice?

4

Where do we stand today?

Honestly, what are our strengths, and where are we exposed?

For more than 30 years, we have helped organizations across the Greater Toronto Area, and throughout Canada, answer exactly these questions. What follows is the same thinking we would walk a client through, without the sales pitch.

The reality every leader is now planning around.

In one recent year, roughly **72% of Canadian small and mid-sized businesses** experienced a cyberattack. The question is no longer whether technology risk affects you. It is whether you have decided how to manage it on purpose, or by accident.

WHERE YOU ARE TODAY

The three ways businesses run IT

Almost every organization runs its technology one of three ways. There is no single right answer: the best fit depends on your size, goals, and how much risk you can carry. But knowing which one you are in is the first step to knowing whether it still fits.

Break-Fix

Reactive

You call someone when something breaks. No monitoring, no plan, just a bill each time. Feels cheap, because you only pay when there is a problem. The catch: you only find out about problems once they have already cost you something.

Internal-Only

Stretched

One or two people "handle IT." This works, until it doesn't. A small team cannot realistically cover security, cloud, compliance, strategy and daily tickets. They become a single point of failure, and strategy gets buried under firefighting.

Managed & Co-Managed

Proactive

A partner monitors your technology around the clock and proactively secures, maintains and plans it as an extension of your team. In a co-managed model, they work alongside your internal staff, taking the heavy lifting so your people focus on the work only they can do.

The shift most growing organizations eventually make is from **reactive** to **proactive**: from paying to fix problems to paying to prevent them.

Reactive	Proactive	Strategic
Break-Fix	Managed / Co-Managed	Technology as advantage

The single-point-of-failure test

If one person on your team won the lottery tomorrow, how much of your technology knowledge walks out the door with them? If the answer makes you uneasy, that is worth a conversation.

THE TRUTH NOBODY PUTS IN A BROCHURE

What you need, and what it costs, is conditional

There is no standard "managed IT package," and no standard price. Anyone who quotes you a flat number before understanding your business is guessing, and you will pay for that guess one way or another.

What you actually need depends on what you already have, the risks specific to your industry, and where you are trying to go. Six factors do most of the work:

1

Size & complexity

Not just headcount: locations, applications, and how much you rely on specialized software.

2

Risk & compliance

PIPEDA applies broadly; Quebec's Law 25 adds more; many industries layer on requirements.

3

What you already have

Modern, well-kept systems need a different engagement than years of deferred fixes.

4

Downtime tolerance

How long can you run if core systems go dark? Lower tolerance means more resilience.

5

Growth & change ahead

Hiring, new locations, mergers and migrations change what you will need 12–24 months out.

6

How strategic you want IT

Kept quietly reliable, or actively driving efficiency and advantage? Both are valid. They cost differently.

The takeaway is not "it is complicated, trust us." It is the opposite: once you understand these six factors for your own business, the right scope and a fair price stop being mysterious. They become a conversation you can have on equal footing.

A fair question to ask any provider

"Before you quote me, what do you need to understand about my business?" A strong partner will have a real answer. A weak one will have a price list.

INSOURCE OR OUTSOURCE

Should you hire IT, or partner for it?

Once you know what you need, the next question is who delivers it. The instinct is that hiring internally must be cheaper than paying a partner. It rarely is. The salary is the most visible cost, not the whole cost, and one person cannot realistically cover security, cloud, compliance, strategy and daily support at once.

The true cost of one internal hire

$90K–$125K base salary alone for an experienced IT generalist in the Toronto area. (Ontario IT salary data, 2026.)

Then add benefits and payroll costs, the monitoring and security licences they need to do the job, tools, and ongoing training and certification: typically another 25% to 40% on top. And after all of it, you still have one person. No after-hours coverage, no bench for vacations or illness, no specialist depth, and a single point of failure if they leave.

A rough guide by size (a starting point, not a rule):

20–50 **Fully outsourced (managed IT).** Rarely enough steady work to justify a full-time hire. A managed partner gives you an entire team, on call, for less than one loaded salary.

50–150 **Co-managed.** One or two internal generalists handle day-to-day requests; a partner covers security, after-hours monitoring, backups and strategy.

150–500 **Co-managed at scale.** An internal team owns the roadmap, with a partner providing 24/7 monitoring, specialized security and surge capacity when projects spike.

The question to actually ask

It is not "employee or vendor?" It is "how do we get every layer covered, affordably, without depending on any one person?" For most organizations under 500 people, some form of partnership is part of a sensible answer.

WHAT IT INCLUDES

What "managed IT" actually covers

The term gets used for everything from a help-desk number to a full strategic partnership. Before you compare options or budgets, know what a complete offering actually includes: five layers.

1. **24/7 monitoring & proactive maintenance.** Systems watched around the clock by a network operations centre; most issues caught before you notice. Fewer problems, not faster apologies.

2. **Security, built in.** Layered protection across endpoints, email and identity, with daily vulnerability scanning, malware protection and patch management, not a later upsell.

3. **24/7 help desk & user support.** Real people your team can reach, with clear expectations for how fast they respond.

4. **Backup, business continuity & disaster recovery.** Geo-redundant, immutable backups and a defined answer to how much data you could lose and how fast you can be back running.

5. **Strategy & planning.** Regular planning against your goals, budgeting for what is coming, staying ahead of risk. The difference between a vendor and an advisor. (Most often the missing layer.)

When you evaluate a provider, map their offer against these five layers. Gaps are not automatically wrong, but they should be your choice, made knowingly, not a surprise you discover during an incident.

Vendor or advisor?

A true managed partner operates as an extension of your team, integrated into how your business runs, not a number you call once something has already broken. Proactive beats reactive every time the lights stay on.

WHAT IT SHOULD COST

Why managed IT has no sticker price

There is a reason no reputable provider will quote you a flat number off a website. What managed IT costs depends on your business, and on top of that, every provider packages it differently. You will see all of these in the market:

- Predictable monthly fee
- Tiered plans
- Priced per user
- Priced per device
- Bundled with other services
- Custom-built package

None of these is automatically better or worse. What matters is the scope behind the number, not the label on it.

The number itself is set by the same six factors from the previous page: your size and complexity, your risk and compliance load, the state of what you already have, your downtime tolerance, your growth, and how strategic you want IT to be. That is why two businesses with the same headcount can land at very different (and equally fair) prices, and why comparing providers means comparing **scope**, not just the monthly figure.

Quality is an investment, not a line item

For most organizations, the cost and disruption of a single serious outage far exceeds the premium for a capable provider. A low monthly fee that leaves out security, strategy or fast support is not cheaper. It is a smaller scope, with the rest of the cost waiting for you down the road. The cheapest quote and the lowest total cost are rarely the same thing.

Reframe the question

Instead of "What does managed IT cost?" ask "What is the right scope for my business, and what should that scope cost?" The first invites a guess. The second gets you an answer you can trust, and a provider worth trusting will welcome the question.

THE BUSINESS CASE

The hidden cost of under-investing

The most expensive IT is usually the IT you under-invested in. The costs do not show up on a monthly invoice. They show up all at once, in the worst week of your year.

$2K–$10K

Typical cost **per hour** of unplanned downtime for a small or mid-sized business, once you add idle payroll, lost revenue and recovery.

Industry downtime estimates, 2025–26

~$640K

Average ransomware **recovery** cost for mid-sized organizations, before any ransom is even considered.

Sophos, 2025

~181

Median number of **days** a breach goes undetected, quietly compounding the damage.

Industry breach data, 2025

The break-fix trap. Paying only when things break feels frugal, but it quietly optimizes for the wrong thing: your provider only earns when something goes wrong, deferred maintenance piles up invisibly, and you carry risk you never agreed to. The point of right-sizing your IT is precisely to make these costs unlikely and survivable, deliberately, before they ever arrive.

Prevention
a predictable monthly investment

One incident
all at once, when you can least afford it

Prevention is not only safer, it is cheaper.

Canadian organizations that fully operationalized security automation reported breach costs roughly **CA$3.3M lower** than those that did not. (IBM Cost of a Data Breach Report, 2025, Canadian data.)

THE RISK ALREADY IN THE BUILDING

Using AI without exposing your business

AI is already inside your business, whether or not you have approved it. Your team uses it to write, summarize, research and draft. Used well, it is a real productivity gain. Used carelessly, it quietly moves your confidential and regulated data into tools you do not own or control.

67% of employees now use AI at work. Only 18% of organizations have a written policy governing it.
Salesforce Workforce AI Survey, 2026.

Breaches that involve unsanctioned "shadow AI" have run roughly US$670K higher than other incidents. (IBM Cost of a Data Breach, 2025.)

What responsible adoption looks like:

1. **A written acceptable-use policy.** Spell out which tools are allowed, for what, and what information must never be entered into them.
2. **Approved, secured tools.** Give people enterprise-grade AI with real data protections, so they stop reaching for free public versions.
3. **Clear data rules.** Client, employee, financial and health information stays out of public models. PIPEDA and Law 25 still apply to it.
4. **Human oversight.** AI drafts and suggests; people review and decide. Nothing leaves the building unchecked.
5. **Training.** Most exposure is accidental. A short, practical session turns the rules into habits and removes most of the risk.

The goal is not to ban AI

It is to capture the upside without inheriting the risk. A simple policy, the right tools and a little training let your team move faster, safely, and keep you on the right side of your privacy obligations.

CHOOSING A PARTNER

What good looks like

Once you know what you need and what it should cost, the last question is who. A strong partner looks the same regardless of size or industry. Use these to evaluate anyone, including the provider you already have.

- **They start with questions, not a quote.** They want to understand your business before they price anything.
- **Security is foundational, not optional.** Protection is built in, with a plan for when, not if, something gets through.
- **They commit to response times in writing.** You know how fast you will get help, and they hold themselves to it.
- **They are proactive by default.** You hear from them when nothing is wrong, not only when something is.
- **They plan with you.** Regular strategy conversations and a roadmap tied to your goals.
- **They speak plainly.** Business terms, not acronyms. You always understand what you are paying for.
- **They show up as a local partner.** They know your business, your people and your context.

Use this as a scorecard.

Score your current provider against all seven. The gaps you find are your agenda for your next renewal conversation, whether that is with them, or with us.

SELF-ASSESSMENT

Is your IT right-sized?

Check each box you can answer "yes" to, honestly. There are no wrong answers, only useful ones.

- [ ] We know exactly what we would lose, in dollars, for every hour our systems are down.
- [ ] Our systems are monitored around the clock, and most issues are caught before we notice.
- [ ] Security (endpoints, email, identity, backups and an incident plan) is built in, not bolted on.
- [ ] We could recover critical data and be running again within a timeframe we have actually decided on.
- [ ] We meet with someone at least quarterly to plan technology against our business goals.
- [ ] We are confident we meet our privacy and compliance obligations (PIPEDA, and Law 25 if applicable).
- [ ] We have a clear, written policy for how our team can and cannot use AI tools, and our people know it.
- [ ] Our IT does not depend on a single person who cannot be replaced quickly.
- [ ] We know what we are paying for, and we understand why each part is there.

8–9 · Strong
Likely right-sized. The opportunity now is optimization and staying ahead.

4–7 · Mixed
Real foundations and real gaps. A focused review shows which gaps matter most.

0–3 · Exposed
More risk and unpredictability than you should carry. Very fixable. Start by seeing the full picture.

Bring your answers to a HubTGI IT Risk Assessment and we will turn them into a clear, prioritized action plan. Free, no obligation.

416-747-1500

YOUR NEXT STEP

Let HubTGI manage your business technologies, so you can focus on running your business.

The natural next step is a HubTGI IT Risk Assessment, a straightforward, no-obligation conversation. We walk through your six factors, look honestly at what you have today, and give you a clear written picture: what you need, what is missing, what it should cost, and what to do first. No pressure, no jargon, just clarity you can act on. We help businesses leverage technology to control costs, boost productivity and secure their data, and make you feel like a customer again.

Book your IT Risk Assessment

hubtgi.com · 416-747-1500
35 Kelfield St., Etobicoke, ON M9W 5A3

hubTGI

ADVANCE2000