THE COST OF REACTIVE IT · 2026

Your IT is "fine." Until the day it isn't.

On a calm day, reactive break-fix IT and fully-managed IT look identical — email opens, files load, nobody calls. Reactive even costs less. That's the trap: "fine" feels like a smart budget call, right up until the one day it isn't — an outage, a locked-up server, a backup that never ran. This brief prices the bet, across industries, and shows how to see your own number before the bad day does.

$8K–$25K

Per-hour cost of downtime for a mid-market firm — ITIC, 2025

88%

Of SMB breaches that involve ransomware — Verizon DBIR, 2025

2 min

To your own IT exposure — no cost, delivered instantly · core12tech.com/it-risk-report

PUBLISHED

August 2026

PREPARED BY

Core12 Tech · Atlanta, GA

FOR

Mid-market · $10M–$200M

CATEGORY

Managed IT & Risk

FINE IS NOT THE SAME AS MANAGED

Nobody notices IT that works. That's exactly the problem.

Every operator knows the feeling of IT that's "fine." Email flows, the ERP's up, tickets get closed eventually. On a calm day, a business running reactive break-fix IT is indistinguishable from one running fully-managed IT — and the reactive one usually costs less month to month. So "fine" reads as the smart cost decision.

It isn't a cost decision. It's a bet. You're wagering that the bad day — the ransomware email someone clicks, the server that finally dies, the backup no one tested — won't land this year. Most years, you win. The year you don't, the savings you banked disappear in a single afternoon, and then some.

The difference between reactive and managed IT isn't visible in how things run. It's visible in what happens when they don't.

02 · THE DIFFERENCE ONLY SHOWS ON THE BAD DAY

What you're actually choosing between

Same result on a good day. On the bad day, only one column has a plan.

REACTIVE · FIX WHEN IT BREAKS

Strategy	No one's watching until something fails.
Cost	Hourly + emergency premiums — highest the week your luck runs out.
Security	Bolt-on, if it's there at all.
Backups	Assumed to be running. Rarely tested.
Response	Best-effort. Measured in hours.

MANAGED · FIX BEFORE IT BREAKS

Strategy	Monitored 24/7; problems caught upstream.
Cost	Fixed monthly — predictable, and lowest on the bad day.
Security	Built into the plan, not billed extra.
Backups	Restores tested on a schedule, not assumed.
Response	Under 10 minutes, guaranteed.

Reactive isn't negligent — it's rational, right up until it isn't. The columns produce the same output on 360 days a year. The business case lives entirely in the other five.

66–80%
Of downtime traces to human error and preventable causes — ITIC

6 in 10
Firms can't calculate what an hour of downtime costs them

181 days
Median time a breach goes undetected — "fine" can already be compromised

A WORKED EXAMPLE

The bad day has a price. Here's the arithmetic.

The figures below model a $30M firm, 85 employees, a $58 average loaded hourly rate, on reactive or light-touch IT. Swap your headcount and rate — the ratios hold. The point isn't the exact dollar. It's that the number is arithmetic rather than opinion, and it's already sitting in your P&L as something else.

WHERE REACTIVE IT QUIETLY BILLS YOU	ASSUMPTION	ANNUAL COST
Unplanned downtime	30 hrs / yr × $8,000 / hr (ITIC low end, 20–100 employees)	**$240,000**
Slow-resolution productivity drain	85 employees × 0.75 hr / wk waiting on IT × 46 wks × $58	**$170,085**
Reactive-IT overspend	Hourly break-fix + emergency premium vs a fixed managed plan	**$93,600**
Conservative annual drag	**Coordination and waste only — excludes any incident**	**≈ $503,685**

Every line is already in your numbers — inside labor cost, inside the IT bill, inside "that was a rough week." None of it is new spend. And it deliberately excludes the number that ends the argument: the bad day itself.

THE DAY IT ISN'T

One ransomware event ≈ $638,536 to recover

That's the average recovery for a firm your size — before any ransom, and before downtime, which typically runs about 50× the ransom itself. Forty percent of mid-market and small firms say a $100K hit alone would put them out of business. (Sophos, 2025 · Verizon DBIR, 2025)

04 · WHY WAITING DOESN'T HOLD THE LINE

- **The hardware you've been lucky with is the hardware that fails.** The five-year-old server that's been "fine" is the single most likely thing to take you down — preventable hardware and human error drive the majority of outages.
- **You can already be breached and not know it.** With a 181-day median dwell time, "we've never had a problem" often just means "we haven't found it yet."
- **Reactive cost creeps up, not down.** Every emergency bills hourly, every renewal renews the same exposure, and the one year you needed a tested backup is the year you learn you didn't have one.

FROM REACTIVE TO MANAGED

You don't need a bad day to find out. Just a baseline.

The fix isn't a bigger IT budget or a panic project the Monday after an outage. It's moving from fix-when-broken to fix-before-it-breaks — and putting a number on the gap first, so the decision is math, not fear.

WEEKS 1–2 · SEE

IT Risk Report

Quantify your downtime, security, compliance, and productivity exposure for your industry and headcount. Output: one exposure number and the three risks most likely costing you right now.

WEEKS 3–8 · STABILIZE

Foundation + Protection

Patching, tested backup and recovery, endpoint and identity, MDR, and 24/7 monitoring. The probability of a bad day drops before anything else about your business changes.

ONGOING · OPTIMIZE

The managed model

Fixed monthly cost, under-10-minute response, a quarterly roadmap, and executive reporting. IT stops being a gamble and becomes a line item you can forecast.

90%
Less downtime — 40+ hrs/yr to under 4, mid-market firms after 12 months

52%
Lower IT operating cost — $180K to $86K on a fixed managed plan

105%
Average ROI on managed IT services — Forrester

06 · BRING THE NUMBER, NOT THE FEAR

Ask in your next leadership meeting

- If we lost email and files for a full day tomorrow, what does it cost — and can anyone in this room name the number?
- When did we last test a restore from backup — not confirm one ran, actually restore from it?
- What's our real response time when something breaks at 4pm on a Friday?

What to ignore

- ✖ Any provider who bills you more the worse your week gets.
- ✖ "We've never had a problem" offered as proof you're covered — that's the definition of the bet.
- ✖ Security sold as a bolt-on instead of built into the plan.

SEE IT BEFORE THE BAD DAY DOES

Get your IT Risk Report — free, instant

Core12's engine quantifies your downtime, security, and compliance exposure on your inputs — not industry averages — and names the three risks most likely costing you now.

Run the IT Risk Report
2 min · no cost · no sales call

Sources. Downtime cost and causes: ITIC 2024–2025 Hourly Cost of Downtime — 20–100-employee firms average $8,000–$25,000/hr, and human error and preventable causes drive 66–80% of incidents. Breach and ransomware: Verizon 2025 DBIR — 88% of SMB breaches involve ransomware, 40% of firms say a $100K incident would be business-ending, 181-day median dwell time. Ransomware recovery: Sophos, State of Ransomware, 2025 — ≈$638,536 average for 100–250-employee firms, excluding ransom. Managed IT outcomes: Forrester (105% ROI) and Core12 Tech client baselines (mid-market, 50–200 employees, 12 months). Worked example is illustrative arithmetic, not a client average.