ELEVATE
SOLUTIONS

GUIDE · IT STRATEGY & OPERATIONS

Why Your Business Needs Managed IT

Break-fix vs. managed

The real cost of DIY IT compared to managed services — cost structure, risk, and what break-fix actually costs when you factor in downtime. Formulas and fill-in worksheets, not invented ROI claims.

01 — THE HIDDEN COST OF BREAK-FIX

What you actually pay when you only pay for repairs

Break-fix looks cheap because the invoice only shows the repair. The larger costs — downtime, deferred maintenance, surprise capital spend, and security drift — never appear on a bill, so they never get counted. This section gives you the formulas to count them.

Start with the structural problem. A break-fix vendor earns revenue when something breaks. The longer and more often your systems fail, the more billable hours exist. That is not an accusation of bad faith — most break-fix technicians do honest work — but the incentive points the wrong way. Nobody in the relationship is paid to prevent the next outage. A managed contract inverts this: the provider collects the same flat fee whether your month is quiet or chaotic, so prevention is how they protect their own margin. Incentive alignment, not technology, is the core difference between the two models.

The five cost categories break-fix invoices never show

COST CATEGORY	WHAT IT LOOKS LIKE IN PRACTICE
Emergency labor rates	Unscheduled work bills at premium hourly rates, often with after-hours multipliers and minimum-hour blocks. You pay the most when you can negotiate the least.
Downtime × payroll	Every hour a system is down, you still pay everyone who depends on it. This is usually the single largest line — and it never appears on any invoice.
Deferred maintenance debt	Patches, firmware, backup tests, and license renewals that nobody owns between visits. The debt compounds quietly until it surfaces as an outage or a breach.
Unbudgeted capital surprises	Hardware runs until it dies, then must be replaced immediately, at whatever price and lead time the market offers that week. No lifecycle plan means no negotiating position.
Security drift	Between visits, accounts go unreviewed, MFA gaps persist, and alerts go unread. Drift is invisible until an incident makes it visible. CISA reports that "Over 90% of successful cyber-attacks start with a phishing email" — a category of failure that prevention and monitoring address and repair visits do not.

The downtime formula

FORMULA

Cost per incident = (hours down × affected employees × average loaded hourly cost) + (hours down × revenue at risk per hour) + emergency labor billed + replacement hardware/software.

Loaded hourly cost per employee = (salary + benefits + employer taxes) ÷ 2,080 working hours. For a quick estimate, multiply base salary by 1.25–1.4 before dividing — label it as your own estimate, not a benchmark.

Worksheet: your most recent significant outage

A — Hours down (detection to full restoration) _____

B — Employees affected (fully or partially idle) _____

C — Average loaded hourly cost per employee ($) _____

D — Idle payroll: A × B × C ($) _____

E — Revenue at risk per hour × A ($) _____

F — Emergency labor billed for the incident ($) _____

G — Hardware/software replaced under duress ($) _____

True incident cost: D + E + F + G ($) _____

Worksheet: your last 12 months of break-fix

All IT vendor invoices, 12 months ($) _____

Number of incidents that idled 3+ people _____

True incident cost (above) × number of incidents ($) _____

Unplanned hardware/software purchases ($) _____

Staff hours spent coordinating IT vendors × loaded rate ($) _____

Annualized true cost of break-fix: sum of the above ($) _____

This annualized figure is the number to carry into Section 02. For regulated firms there is a second, larger number lurking behind it: incident cost when the failure involves data. Organizations under 500 employees: average $3.31M per breach. IBM Cost of a Data Breach Report 2023 No worksheet line absorbs that — it is the risk the maintenance debt and security drift rows are quietly accumulating.

02 — MANAGED SERVICES ROI

What actually changes under a managed contract

Managed services do not make IT cheaper in every case. What they change is the cost structure: variable and unbounded becomes flat and budgetable, and prevention becomes someone's paid job. Here is what moves, and an honest account of when it isn't worth it.

DIMENSION	BREAK-FIX	MANAGED
Labor	Hourly, premium rates for emergencies, billed per incident	Covered under a flat monthly fee for in-scope work; emergencies don't generate new invoices
Monitoring & patching	None between visits; problems found when they hurt	Continuous monitoring and a scheduled patching baseline; many failures caught before users notice
Lifecycle planning	Hardware runs to failure; replacement is an emergency	Tracked asset ages and warranty dates; replacements scheduled and budgeted a fiscal year ahead
Security stack	Whatever was installed last visit; drift between visits	A defined baseline (endpoint protection, MFA enforcement, backup verification) maintained as part of the service
Budget	Unpredictable; spikes follow failures	Flat monthly figure plus a planned project list; finance can forecast it

The speed difference matters most where data is involved. Detection and containment time drives breach cost directly: breaches contained <200 days averaged $3.61M vs $5.49M for >200 days. IBM Cost of a Data Breach Report 2025 The mean across all organizations is 241 days to identify and contain. IBM Cost of a Data Breach Report 2025 Continuous monitoring exists to pull your firm toward the short side of that split. A vendor you call after the fact cannot.

Run the comparison yourself

> **FORMULA**
>
> Annual managed cost = (monthly fee × 12) + onboarding fee (year one) + quoted out-of-scope projects. Compare against the annualized true cost of break-fix from Section 01 — not against last year's invoices alone. The invoices are the visible third of the iceberg.

Quoted monthly fee × 12 ($) _____

One-time onboarding fee ($) _____

Expected out-of-scope projects, year one ($) _____

Annual managed cost ($) _____

Annualized true cost of break-fix, from Section 01 ($) _____

If the managed number is higher, the remaining question is what you are buying for the difference: shorter outages, a maintained security baseline, a capital plan, and — for regulated firms — documentation you can hand to an auditor, a carrier, or opposing counsel. Price that against your actual exposure, not against a generic ROI percentage. Any provider quoting you a precise ROI figure for your firm without seeing your environment is guessing.

> **WHEN BREAK-FIX IS FINE**
>
> Be honest about the cases where managed services are the wrong buy. If you run five seats or fewer, hold no regulated or client-confidential data, depend on standard cloud apps a consumer could reset, and can genuinely tolerate a day or two of downtime without losing revenue or clients — break-fix with a competent local technician is a defensible choice. The math in this guide will likely confirm it. Managed contracts earn their fee where downtime is expensive, data is sensitive, or a regulator can ask what your controls were on a given date. If none of those describe you, keep the cash.

03 — WHAT TO LOOK FOR IN AN MSP

The 10-item evaluation checklist

Deciding the model is half the work; the provider is the other half. Put these ten items to every provider you evaluate — no exceptions — and insist on answers in writing. A provider who resists writing things down before the contract will not improve afterward.

- [ ] **Documented onboarding process** 1
  Ask for the actual onboarding plan: discovery, asset inventory, credential transfer, baseline remediation, and a stated timeline. "We'll figure it out" is a no.
- [ ] **Response-time definitions in writing** 2
  Documented response times by severity level, with definitions of what counts as critical, and how response time is measured (acknowledgment vs. work started vs. resolution).
- [ ] **Security baseline included, not upsold** 3
  Get the line-item list of what the base fee covers: endpoint protection, MFA enforcement, patching, backup verification, email filtering. Anything security-critical sold as an add-on is a structural red flag.
- [ ] **Regulated-industry experience** 4
  If you answer to HIPAA, state bar rules, SEC/FINRA, or insurance carriers, ask which frameworks they support today and what audit evidence they can produce. Ask for a sample compliance report, redacted.
- [ ] **References from firms like yours** 5
  Two or three current clients of similar size and industry. Ask the references about the worst incident, not the best month — how it was handled, how it was communicated, what changed afterward.
- [ ] **Offboarding and data-return terms** 6
  Before you sign, know how you leave: documentation handover, admin credential transfer, data export format, and timeline — in the contract, not a verbal assurance. Good providers make leaving easy; that is exactly why you can stay.
- [ ] **Stack transparency** 7
  They should name the actual tools they run for monitoring, backup, and endpoint security, and tell you who holds the licenses and the data if you part ways. "Proprietary platform" with no specifics deserves follow-up questions.
- [ ] **Quarterly business review cadence** 8
  A standing QBR with an agenda: incident trends, asset lifecycle, upcoming budget items, and open risks. If reviews only happen when you complain, planning isn't happening either.
- [ ] **Co-managed option** 9
  If you have internal IT staff, ask whether the provider can work alongside them with split responsibilities in writing. A provider that insists on all-or-nothing is optimizing for their model, not your firm.
- [ ] **Local onsite capability** 10
  Some failures — hardware, network closets, conference rooms before a hearing or a closing — require hands on site. Ask where their nearest technicians sit and what onsite dispatch looks like for your address.

HOW TO USE THIS LIST

Send all ten items to every finalist as written questions and compare the answers side by side. Score answers, not presentations. A provider that answers eight in writing beats one that answers ten over lunch. Keep the responses — they become the baseline you hold the winner to at the first quarterly review.

ELEVATE SOLUTIONS

Elevate Solutions provides managed IT and cybersecurity for businesses that answer to regulators, clients, and courts.

Elevate Solutions

6230 Wilshire Blvd Suite 2120, Los Angeles CA 90048

(424) 400-6625 · support@elevatesolutions.io · elevatesolutions.io