The ROI of Managed IT Services

A Data-Driven Analysis

Quantifying the Business Value of Outsourcing IT Operations to a Managed Services Provider

Published Q1 2024
ComDirect USA
comdirectusa.com

Table of Contents

Chapter 1

The Real Cost of Doing IT In-House

Most organizations dramatically underestimate the true cost of running IT internally. The salary line item on the budget is visible, but it represents only a fraction of the total investment. When you add up the hidden costs, the fully loaded cost of in-house IT is typically 1.5 to 2.5 times the salary budget alone.

Visible Costs

- IT staff salaries and benefits (health insurance, retirement, PTO)
- Hardware: servers, switches, firewalls, access points, UPS systems, and end-user devices
- Software licensing: operating systems, productivity suites, security tools, monitoring platforms, backup solutions
- Internet circuits and telecom services
- Data center or server room costs (power, cooling, physical security, rack space)

Hidden Costs

- Recruiting: the average cost to hire a single IT professional is $15,000-$25,000 when accounting for recruiter fees, job board postings, interview time, and onboarding
- Training and certifications: keeping staff current on evolving technologies costs $3,000-$8,000 per person per year
- Turnover: the IT industry averages 13-15% annual turnover. Each departure triggers a new recruiting cycle and months of reduced productivity
- Coverage gaps: a two-person IT team has no coverage during vacations, sick days, or after hours without overtime pay
- Opportunity cost: IT staff pulled into break-fix work cannot execute strategic projects that drive business value

The Coverage Problem

A mid-market company with 150 employees and a 3-person IT team has approximately 6,500 annual hours of IT labor. After meetings, administration, vacations, and sick time, roughly 4,500 productive hours remain. Industry benchmarks suggest that a 150-person environment generates 4,000-5,000 support tickets per year, leaving almost no capacity for infrastructure improvements, security hardening, or strategic projects.

Chapter 2

What Managed IT Services Actually Includes

Managed IT services is a broad term that covers a range of engagement models. Understanding what is included, and what is not, is essential for accurate cost comparison.

Core Managed Services (Typically Included)

- 24/7/365 monitoring of servers, network devices, endpoints, and cloud infrastructure
- Help desk support for end users (phone, email, chat, and remote control)
- Patch management: OS and application updates tested and deployed on a defined schedule
- Backup management: daily verification, test restores, and retention policy enforcement
- Endpoint security: antivirus/EDR deployment, management, and incident response
- Vendor management: coordinating with ISPs, SaaS vendors, and hardware suppliers on your behalf
- Documentation: maintaining network diagrams, asset inventories, and runbooks

Enhanced Services (Often Available as Add-Ons)

- Virtual CIO/CTO: strategic technology planning, budgeting, and roadmap development
- Advanced cybersecurity: SIEM/SOC, vulnerability management, penetration testing, compliance support
- Cloud management: architecture, migration, optimization, and cost management for AWS/Azure/GCP
- Project work: office moves, infrastructure upgrades, new site deployments, application rollouts

Engagement Models

- All-inclusive (per-user or per-device): fixed monthly fee covers all support and management. Most predictable model.
- Tiered: base monitoring and management with support hours capped or charged per incident above a threshold
- Co-managed: MSP augments your existing IT team, filling gaps in coverage, expertise, or tooling

The Co-Managed Model

Co-managed IT is increasingly popular among mid-market companies that have internal IT staff but lack depth in areas like cybersecurity, cloud, or compliance. The MSP provides the tooling platform, 24/7 monitoring, and specialized expertise while the internal team retains control of strategy and day-to-day user relationships.

Chapter 3

Total Cost of Ownership: In-House vs. Managed

The most meaningful comparison is total cost of ownership (TCO) over a 3-5 year period. TCO accounts for all direct and indirect costs, including those that organizations frequently overlook when building in-house budgets.

TCO Comparison: 150-Employee Organization

The following comparison uses industry benchmark data for a mid-market organization with 150 employees, 10 servers, and standard business applications.

Cost Category	In-House (Annual)	Managed (Annual)
IT Staff (3 FTEs + benefits)	$330,000	Included
Recruiting & Turnover	$25,000	N/A
Training & Certifications	$18,000	N/A
Security Tools & Licensing	$45,000	Included
Monitoring & Management Tools	$24,000	Included
Backup & DR Solutions	$18,000	Included
After-Hours Coverage (OT)	$30,000	Included
Hardware Refresh (Amortized)	$60,000	$60,000
Internet & Telecom	$36,000	$36,000
MSP Monthly Fee	N/A	$180,000
Estimated Annual Total	**$586,000**	**$276,000**

In this benchmark scenario, managed services delivers a 53% reduction in total IT operating cost. The primary drivers are staff consolidation (the MSP spreads its team across multiple clients, sharing the cost of specialized expertise), included tooling (enterprise-grade platforms amortized across the MSP's client base), and elimination of recruiting and turnover costs.

Important Caveat

Every organization is different. The figures above are industry benchmarks, not guarantees. Your actual TCO depends on your environment complexity, compliance requirements, geographic distribution, and the specific MSP engagement model. The calculation framework in Chapter 10 will help you build your own comparison.

Chapter 4

Downtime Costs and Uptime Guarantees

Downtime is the single most expensive IT failure, and it is where managed services delivers its most dramatic ROI. The cost of downtime varies by industry, but the pattern is consistent: unplanned outages are devastatingly expensive.

The Cost of Downtime

Industry research consistently estimates the average cost of IT downtime at $5,600 per minute for mid-market organizations. This figure includes:

- Lost revenue: transactions that cannot be processed, orders that cannot be placed
- Lost productivity: employees who cannot work because systems are unavailable
- Recovery costs: overtime labor, emergency vendor fees, expedited hardware replacement
- Reputational damage: customer dissatisfaction, missed SLAs, lost future business

In-House vs. Managed Response Times

The critical difference is not whether outages occur, but how quickly they are detected and resolved:

- In-house (reactive): Problems are often discovered when users report them. Mean time to detect (MTTD) can be 30-60 minutes for after-hours incidents. A 3-person team has no on-call rotation without burnout.
- Managed (proactive): 24/7 monitoring detects issues in seconds. Automated alerts trigger immediate response. NOC teams begin remediation before users are affected. MTTD drops to under 5 minutes.

The difference in annual downtime is significant. Industry data shows that organizations using proactive managed services experience 50-70% less unplanned downtime than those relying on reactive in-house support. For a company that experiences 10 hours of unplanned downtime per year at $5,600 per minute, reducing that to 3 hours saves $2.35 million annually.

SLA-Backed Uptime

Reputable MSPs back their monitoring with SLA-guaranteed response times: typically 15 minutes for critical issues and 1-4 hours for standard requests. In-house teams rarely formalize SLAs with the business, making it difficult to measure and improve response performance.

Chapter 5

Security ROI: Breach Prevention Economics

Cybersecurity is where the ROI equation for managed services becomes most compelling. The cost of a security breach dwarfs the cost of prevention, and most small-to-mid-market organizations cannot afford to build an enterprise-grade security operation internally.

The Cost of a Breach

Industry breach cost studies consistently report:

- Average total cost of a data breach: $4.45 million (all industries)
- Average cost for organizations under 500 employees: $3.31 million
- Average cost per compromised record: $165
- Mean time to identify and contain a breach: 277 days
- Organizations with incident response plans and tested playbooks save an average of $1.49 million per breach

What an MSP Security Stack Provides

A managed security stack typically includes capabilities that would cost $200,000-$400,000 annually to build in-house:

- Endpoint Detection and Response (EDR) with 24/7 SOC monitoring
- SIEM log aggregation and correlation with automated alerting
- Email security: advanced phishing protection, URL detonation, attachment sandboxing
- Vulnerability scanning and patch management on a defined cadence
- Security awareness training for all employees
- Incident response planning, tabletop exercises, and breach response support

The Multiplier Effect

An MSP's security team monitors thousands of endpoints across hundreds of clients. When a new threat is detected at one client, the response, including indicators of compromise, detection rules, and remediation procedures, is immediately deployed across the entire client base. This collective defense model provides threat intelligence and response speed that no single mid-market organization can replicate internally.

Insurance Impact

Cyber insurance carriers increasingly require specific security controls (MFA, EDR, backup verification, incident response plans) as conditions of coverage. Organizations using managed security services often qualify for lower premiums because these controls are already in place and continuously monitored. Premium reductions of 10-25% are common.

Chapter 6

Staffing Economics and the IT Talent Gap

The IT talent shortage is not a temporary market condition. It is a structural reality that fundamentally changes the economics of in-house IT. Understanding these dynamics is essential for any honest ROI analysis.

The Talent Gap by the Numbers

- Industry workforce studies estimate a global shortage of 3.4 million cybersecurity professionals
- The average time to fill an IT position is 45-60 days, during which the role goes unfilled or is covered by remaining staff at the expense of other priorities
- IT salary inflation has outpaced general wage growth by 2-3x over the past five years
- Remote work has nationalized the talent market: a company in a mid-tier city now competes with employers in San Francisco, New York, and fully remote positions

The Specialization Problem

Modern IT requires deep specialization across multiple domains: networking, cloud architecture, cybersecurity, compliance, endpoint management, and collaboration platforms. A 3-person IT team cannot maintain expert-level knowledge across all of these areas. The result is one of two outcomes:

- Generalists who know a little about everything but lack the depth to handle complex issues, leading to longer resolution times, suboptimal architectures, and security gaps
- Specialists who are strong in one area but leave other domains under-served, creating blind spots that manifest as outages, breaches, or failed audits

The MSP Staffing Model

An MSP distributes the cost of specialized talent across its entire client base. A 50-person MSP serving 100 clients can employ dedicated specialists in networking, security, cloud, and compliance, giving each client access to expert-level support in every domain at a fraction of the cost of hiring those specialists directly.

Key Insight

The question is not whether you can afford managed services. The question is whether you can afford to compete for scarce IT talent against every other employer in the country, pay market-rate salaries for specialists you need 10 hours per month, and absorb the cost and disruption of 13-15% annual turnover, all while keeping the lights on and executing strategic projects.

Chapter 7

Scalability Without Capital Expenditure

Business growth should not be gated by IT infrastructure. One of the most significant but least quantified benefits of managed services is the ability to scale IT operations without large capital expenditures or long lead times.

The Capital Problem with In-House IT

Scaling in-house IT requires capital investment in advance of need:

- New office location: $50,000-$150,000 for network infrastructure, server room, and endpoint deployment, plus 60-90 days of lead time
- Headcount growth: each new employee requires a provisioned workstation, accounts, security configuration, and ongoing support capacity. At scale, you need additional IT staff.
- New application deployment: often requires server capacity, licensing, integration work, and ongoing management that was not budgeted when the application was approved
- Acquisition integration: merging IT environments is a 6-18 month project that consumes the entire IT team while day-to-day operations still need to run

How Managed Services Scales

- Per-user pricing: costs scale linearly with headcount. Adding 50 employees adds a predictable monthly cost with no capital outlay for tooling or infrastructure.
- New site deployment: MSPs maintain standardized deployment playbooks and pre-staged equipment. A new office can be operational in days, not months.
- Elastic expertise: need a cloud architect for a migration project? A compliance specialist for an audit? The MSP provides the expertise without a permanent hire.
- Acquisition support: the MSP has done IT integrations before and can run the technical workstream while your internal team stays focused on business integration.

Growth-Stage Companies

For companies growing 20%+ annually, managed services is often the only viable path. Hiring and training IT staff fast enough to keep pace with business growth is impractical. The MSP model lets IT capacity scale at the speed of the business rather than the speed of recruiting.

Chapter 8

Predictable Budgeting and Cost Containment

CFOs and finance teams value predictability. In-house IT spending is notoriously volatile: an unexpected server failure, a security incident, or a critical hire that takes six months to fill can blow the budget in a single quarter. Managed services converts this volatility into a predictable monthly operating expense.

The Volatility of In-House IT Costs

- Hardware failures: a single server or firewall failure can cost $10,000-$50,000 in emergency replacement and recovery labor
- Security incidents: breach response costs (forensics, legal, notification, remediation) average $3.3 million for mid-market organizations
- Staff turnover: an unexpected departure costs $15,000-$25,000 in recruiting plus months of knowledge loss
- Emergency projects: a compliance audit finding or critical vulnerability can force unbudgeted remediation projects

The Managed Services Budget Model

A well-structured MSP agreement provides:

- Fixed monthly fee covering all monitoring, management, and support for the defined scope
- Hardware-as-a-service options that spread refresh costs into the monthly fee, eliminating capital expenditure spikes
- Included security stack that removes the risk of surprise incident costs for covered events
- Defined project rates for out-of-scope work, providing cost certainty even for discretionary projects
- Annual technology budget planning with vCIO guidance that aligns IT spending with business priorities

Budget Variance

Organizations using in-house IT typically see 15-30% variance between budgeted and actual IT spending annually. Organizations using all-inclusive managed services report variance below 5%, driven almost entirely by discretionary project work that was approved in advance.

Chapter 9

Productivity Gains and Employee Experience

IT ROI is not only about cost reduction. It is also about the productivity of every employee who depends on technology to do their work, which in most organizations means everyone.

The Cost of IT Friction

Every minute an employee spends wrestling with technology is a minute they are not doing their actual job:

- The average employee loses 22 minutes per day to IT-related issues (slow systems, login problems, application errors, printer jams)
- At a fully loaded cost of $50/hour, that represents $2,750 per employee per year in lost productivity
- For a 150-person organization, that is $412,500 annually in productivity loss from IT friction

How Managed Services Reduces Friction

- Proactive monitoring catches and resolves issues before users are affected: disk space alerts, memory leaks, expiring certificates, and failing hardware are addressed during maintenance windows
- Professional help desk with defined SLAs: users get consistent, timely support rather than waiting for an available internal resource
- Standardized environments: consistent configurations reduce the "it works on my machine" problems that consume troubleshooting time
- Self-service portals: password resets, software requests, and common tasks are automated, reducing ticket volume and wait times

Employee Satisfaction and Retention

IT experience directly impacts employee satisfaction. Employees who rate their IT experience as "poor" are twice as likely to report dissatisfaction with their employer. In a competitive labor market, IT friction is an employee retention risk that shows up in HR metrics, not IT metrics. A managed services partnership that delivers reliable, responsive technology support improves the daily experience of every employee in the organization.

The 22-Minute Problem

Reducing daily IT friction from 22 minutes to 10 minutes per employee, a realistic target with proactive managed services, recovers $206,000 in annual productivity for a 150-person organization. That single metric often exceeds the net cost difference between in-house and managed IT.

Chapter 10

How to Calculate Your Own MSP ROI

The benchmarks in this paper provide useful reference points, but the decision to engage managed services should be based on your own numbers. Use the framework below to build a TCO comparison specific to your organization.

Step 1: Calculate Your In-House IT Costs

- Staff costs: salaries + benefits (typically 1.3-1.4x salary) for all IT personnel
- Recruiting costs: average cost per hire multiplied by annual turnover rate
- Training: certifications, conferences, courses for each team member
- Tools and licensing: list every security, monitoring, backup, and management tool and its annual cost
- Hardware: amortize all infrastructure over its expected lifespan (typically 3-5 years)
- Facilities: allocate server room costs (power, cooling, space, physical security)
- After-hours coverage: overtime, on-call stipends, or the cost of not having coverage

Step 2: Estimate Hidden and Risk Costs

- Downtime: multiply your average hours of unplanned downtime by your per-hour downtime cost
- Security incidents: multiply breach probability by average breach cost for your industry and size
- Productivity loss: estimate daily IT friction minutes per employee, convert to annual cost
- Opportunity cost: estimate the revenue impact of delayed strategic projects due to IT capacity constraints

Step 3: Get MSP Quotes

Request detailed proposals from 2-3 MSPs. Ensure quotes are scoped to your actual environment and include:

- What is included in the base fee vs. what is billed as additional
- SLA commitments for response and resolution times
- Onboarding and transition costs
- Contract term, escalation clauses, and termination provisions

Step 4: Compare and Decide

Build a 3-year TCO model comparing your fully loaded in-house costs (Steps 1+2) against the MSP proposals (Step 3). Factor in qualitative benefits that are difficult to quantify: access to specialized expertise, reduced risk exposure, scalability, and the ability to redirect internal IT resources toward strategic initiatives.

About ComDirect USA

ComDirect USA is a full-service technology partner specializing in enterprise infrastructure, cybersecurity, cloud architecture, and managed IT services. With offices in Irvine, California, and Meridian, Idaho, we serve organizations across healthcare, legal, financial services, manufacturing, and logistics.

Contact Us

Phone: 949.208.8800 | Toll Free: 800.733.7030

Email: info@comdirectusa.com

Web: comdirectusa.com