spector IT

Traditional IT Support is SHIT

Why is that and what to do about it

Traditional IT Support is Shit. **3**

Traditional IT Support is Shit.

And You Already Know It.

Why the average business suffers for years with broken IT before someone finally asks: ***"Why are we putting up with this?"***

1. The Uncomfortable Truth

Here's a number that should make every business owner uncomfortable: the average MSP client tenure is **7.6 years**. That's not loyalty. That's inertia.

Think about that for a moment. Nearly eight years with the same IT provider. Through bad service. Through surprise bills. Through 2am calls that shouldn't have happened. Through breaches that could have been prevented. Through that creeping, nagging feeling that things aren't right — but the pain of switching feels worse than the pain of staying.

Sound familiar? You're not alone. A CloudBolt Software report found that **80% of MSP customers are so frustrated with their provider that they're actively looking to replace them**. Let that sink in. Four out of five businesses are unhappy with their IT support. And yet most of them won't actually leave. Not this year. Probably not next year either.

Why? Because changing IT provider feels like moving house while the house is on fire. It's disruptive, it's risky, and nobody has time for it. So businesses tolerate. They cope. They normalise the dysfunction. The IT manager learns to work around the gaps. The CEO stops asking questions because the answers are always in jargon they don't understand. And the MSP? They keep billing.

> **80% of MSP customers are so frustrated they're actively looking to replace their provider.**
> *— CloudBolt Software, Service Provider Industry Report*

The ScalePad 2025 MSP Business Trends Report paints an equally damning picture: **36% of MSPs have customer retention rates below 50%** — meaning they're losing half their clients annually. And yet only **34% of MSPs even bother to track Customer Lifetime Value or churn rates**. They don't measure it because they don't want to know.

2. Why Traditional IT Support Stays Shit

This isn't about individual technicians being bad at their jobs. The problem is structural. The traditional MSP model is *designed* to be reactive, and reactive IT is a losing proposition for everyone except the provider.

The Break-Fix Trap

Most traditional IT support still operates on what the industry calls a "break-fix" model. Something breaks. You call. They fix it. They bill you. Repeat. The fundamental incentive is backwards — your MSP profits from your problems. They have no commercial motivation to *prevent* the fires because fighting fires is what keeps the invoices flowing.

ConnectWise's own research confirms this: the MSPs that have shifted to proactive, prevention-first models achieve better margins, lower technician burnout, and stronger client trust. Yet the majority of the industry remains stuck in the reactive cycle because it's easier to sell "unlimited support" than to genuinely reengineer how IT gets delivered.

The "Unlimited Support" Lie

Ah yes, "unlimited support." The three words that should trigger immediate scepticism in any business owner. As one Reddit user on r/smallbusiness put it: *"MSPs claim unlimited support but when you read the fine print, there are many exceptions that will generate unexpected bills."*

This is the MSP industry's dirty secret. The headline price gets you in the door. Then come the exclusions: after-hours work, project-based changes, new user setups, hardware procurement — suddenly your "unlimited" plan has more limits than a budget airline. ConnectWise's State of SMB Cybersecurity 2025 report found that **58% of SMBs spent more on cybersecurity in 2024 than originally anticipated**. The budgets they were sold didn't match the reality they received.

The Vendor-Induced Chaos

Here's what really breaks IT managers. It's not just that their MSP is reactive — it's that the entire vendor ecosystem treats them as unpaid beta testers. In 2025 alone, the r/sysadmin community documented Windows Server 2022 being accidentally upgraded to 2025 via a mislabelled update (creating licensing nightmares), DHCP services broken by Patch Tuesday, RDP sessions frozen after cumulative updates, and 802.1X authentication failures after Windows 11 24H2 rollouts.

A good MSP should be the firewall between vendor chaos and your business operations. They should test updates before deploying them. They should have staged rollout procedures. They should catch the problems before you do. Instead, most MSPs push updates through blind and wait for the phone to ring.

The Talent Drain

MSPs competing on price create environments that burn through technicians like disposable batteries. High turnover means the person who understood your network last month has been replaced by someone starting from scratch this month. The ScalePad research shows that MSPs with high staff utilisation rates and formal customer success programs dramatically outperform their peers — but these are the minority, not the norm. The result for you? A different technician every

time you call, no continuity, no institutional knowledge of your systems, and the constant feeling that you're explaining yourself for the first time.

> **Only 34% of MSPs track Customer Lifetime Value or churn rates.**
> *— ScalePad 2025 MSP Business Trends Report*

3. What It's Actually Costing You

Let's stop talking about frustration and start talking about money. Because the real cost of shit IT support isn't the monthly invoice — it's everything that invoice fails to prevent.

The Breach You Haven't Had Yet

ConnectWise's 2025 State of SMB Cybersecurity report found that **57% of SMBs now rank cybersecurity as their number one business priority**, up from 43% in 2024. And **83% acknowledge that AI and generative AI are increasing their threat level**. Yet only 51% have actually implemented related security policies. The gap between awareness and action is where breaches happen.

The numbers are brutal. According to IBM's Cost of a Data Breach Report 2025, the average breach now costs **$4.88 million globally**. For SMBs specifically, Kaseya's 2025 data puts the average phishing-related breach at **$140,000** — a 13% increase in just one year. NinjaOne, citing ConnectWise research, reports that **78% of SMBs fear a major incident could put them out of business entirely**.

And here's the kicker: **70% of SMBs are still relying on traditional antivirus and firewalls as their primary defence**. That's like fitting a bicycle lock to a bank vault. AI-powered attacks rose 47% in 2025. The attackers have upgraded. Most MSPs haven't upgraded their clients.

> **47% of small businesses (under $10M revenue) were hit by ransomware in the last year.**
> *— FBI Internet Crime Report 2024 / ConnectWise*

The Downtime You're Absorbing

Every hour your systems are down costs you revenue, productivity, and customer trust. Research shows that **32% of SMBs say less than one day of downtime could critically damage their business**. And yet most traditional MSPs are monitoring your systems the same way a security guard monitors a building by only checking in when someone trips an alarm.

Proactive monitoring — the kind that catches a failing drive before it takes out your file server, that identifies unusual network traffic at 3am before ransomware encrypts everything by 9am — is technically straightforward. It's not expensive. But it requires an MSP that genuinely invests in

prevention rather than response. ConnectWise's research confirms that prevention-led strategies reduce both incident frequency and technician burnout, creating what they call "long-term partnerships and higher client retention." The MSPs doing it well know this. The rest haven't changed because they haven't had to.

The Compliance Exposure

GDPR. NIS2. ISO 27001. PCI DSS. The regulatory landscape is getting more complex every year, and the penalties for non-compliance are getting steeper. Research shows that non-compliance adds an average of **$174,000 to the cost of a breach**. Meanwhile, 69% of organisations find regulations too complex or numerous to navigate, and 69% fail at least one compliance audit annually.

Your traditional MSP probably isn't helping you with this. They're too busy fighting the fires they should have prevented to think about your compliance posture. And the business opportunities you're missing — the enterprise clients who require ISO 27001, the tenders that demand NIS2 compliance — represent revenue you'll never see because your IT partner can't think beyond the next support ticket.

4. The New Hire Effect: Why Change Almost Always Comes From Outside

Here's the pattern we see repeatedly, and it's backed by years of industry data: businesses don't leave bad MSPs because they've decided things should be better. They leave because **someone new walks through the door**.

A new Operations Director. A new CTO. A new Finance Director who actually reads the IT invoices. Someone who hasn't spent years normalising the dysfunction. They arrive, they look at the IT setup, and within a week they're asking the question nobody else had the energy left to ask: *"Why are we paying for this?"*

The Axcient research quantifies part of this: **23% of SMBs would leave their provider over IT service quality issues**, and **48% cite device performance problems as the top factor that would trigger a switch**. These aren't obscure issues. They're the everyday frustrations that existing staff have learned to tolerate but fresh eyes find intolerable.

Even more telling: Montra Technologies reports that **nearly one in four SMBs (24%) have already changed MSPs in the aftermath of a cyberattack**. It shouldn't take a breach to force a change. But for many businesses, it does — because the existing team has been worn down, the CEO doesn't know what good looks like, and the MSP has successfully made itself appear indispensable simply by being complicated.

You don't need to hire someone new to have this realisation. You just need to ask yourself the questions a new hire would ask: Is our IT actually protecting us? Can I budget with confidence? Do I understand what I'm paying for? Is my IT team empowered or frustrated? If the answers are uncomfortable, it's time.

> **24% of SMBs changed MSPs after experiencing a cyberattack. It shouldn't take a breach to force change.**
> *— Montra Technologies*

5. What The Industry Itself Knows (But Won't Tell You)

The irony is that the MSP industry's own research confirms everything we're saying. These aren't outsider criticisms — these are the findings from the platforms and vendors that MSPs themselves rely on.

ConnectWise — arguably the largest platform serving MSPs globally — has published extensively on the gap between what MSPs promise and what they deliver. Their 2025 reports confirm that profitability became the top performance indicator among growing MSPs, but that growth without operational efficiency proved unsustainable. They found a growing divide between MSPs with disconnected tools and those embracing integrated, automated systems. Their data shows that transparency builds loyalty, and that providers sharing real-time dashboards earn higher retention and grow faster through referrals.

Pax8's 2025 Agentic Inflection Point report goes further: they argue the traditional MSP model is *reaching maturity* — their diplomatic way of saying it's becoming obsolete. Their survey found that 66 Pax8 partners believe they'll be seen as strategic business advisors within two years, representing a seven-fold increase from their current role as reactive IT support. The shift from vendor to advisor isn't aspirational — it's already happening. The question is whether your MSP is making that shift.

ScalePad's 2025 research is perhaps most damning for the traditional model. They found that MSPs with the highest revenue and customer satisfaction share specific characteristics: formal customer success programs, client-facing technology roadmaps, vCIO and vCISO services, and proactive monitoring of multiple financial and operational metrics. The best MSPs look nothing like traditional IT support. They look like strategic partners. The question for every business owner is simple: does your current provider look like the top performers, or the bottom 36% who are losing half their clients every year?

6. What “Not Shit” Actually Looks Like

So what does modern IT support look like when it’s done properly? It’s not complicated, but it does require a fundamentally different approach to the break-fix model most businesses are stuck with.

Proactive, Not Reactive

Genuine 24/7 monitoring that catches and resolves issues before they impact your business. Not the “monitoring” that many MSPs claim to offer but which really just means they’ll see the alert when they check their dashboard on Monday morning. ConnectWise’s research shows that prevention-led strategies deliver measurable ROI through downtime avoided and issues prevented. Your IT partner should be proving this to you with data, not just telling you everything’s fine.

Transparent Pricing That Doesn’t Move

One predictable monthly cost. No surprise invoices. No “unlimited support (terms apply).” The ConnectWise research consistently shows that pricing transparency is one of the strongest predictors of client retention. If your MSP can’t give you a flat, honestnumber that covers everything, they’re either hiding costs or they don’t understand their own service delivery well enough to price it properly. Both are problems.

Modern Security That Matches Modern Threats

EDR (Endpoint Detection and Response), AI-powered threat detection, SOAR (Security Orchestration, Automation and Response), and zero-trust architecture. These aren’t luxury add-ons — they’re the baseline for defending against 2026’s threat landscape. Only 11% of SMBs currently use AI-powered security tools. The 89% who don’t are bringing a knife to a gunfight.

Business Language, Not Jargon

Your IT partner should be able to explain every risk, every investment, and every decision in terms your CEO and your board can understand. Revenue exposure. Compliance implications. Competitive impact. If the only people who understand your IT reports are other IT people, your provider is failing you. Pax8’s research confirms this shift is already underway — the best MSPs are repositioning as strategic advisors who drive business outcomes, not just technology vendors who fix broken things.

Tested Updates and Staged Rollouts

No more 2am calls because a vendor pushed a broken update to your production environment. Proper change management means testing patches before deployment, rolling them out in stages, and having a rollback plan when things go wrong. This is basic operational hygiene, and yet the majority of MSPs still push updates blind and hope for the best.

7. The Real Question: Can You Afford To Stay?

We've laid out the data. The CloudBolt research showing 80% frustration. The ConnectWise reports confirming the gap between promise and delivery. The ScalePad data revealing that a third of MSPs can't even retain half their clients. The Pax8 analysis declaring the traditional model obsolete. The IBM, Kaseya, and FBI data quantifying what a breach actually costs.

The question isn't whether traditional IT support is failing businesses. The industry's own research proves it is. The question is how much longer you're willing to be one of those businesses.

Every month you stay with an underperforming MSP is a month where your systems are more vulnerable than they need to be. Where your IT team is more frustrated than they should be. Where your CEO is paying for services they don't fully understand and aren't fully receiving. Where a preventable incident is one phishing email away from becoming a business-ending crisis.

You don't need to wait for a new hire to walk in and state the obvious. You don't need to wait for a breach to force your hand. You need **someone to look at your IT with fresh eyes and tell you, honestly, where the gaps are** — in language that both your IT team and your CEO can understand.

GET A FRESH Perspective

Score yourself on our self-assessment

Our IT Support Checklist is designed to give you an honest picture of where you IT support stands right now. Complete it in a team meeting, or hand it to a colleague and compare answers. Your impression could be completely different to the typical team members.

Share your completed checklist with your IT provider and ask them to respond to the areas where you scored lowest. A good provider will welcome the conversation. If they get defensive or dismissive, that tells you something too.

It's free. It quick and will provide value, guaranteed.

spector.ie/IT-Support-Checklist

For more information keep an eye on our blog.

Sources & References

- CloudBolt Software — Service Provider Industry Report (2022): 80% MSP customer frustration statistic
- ConnectWise — The State of SMB Cybersecurity 2025 (Vanson Bourne research): AI threat levels, cybersecurity spending, SMB priorities
- ConnectWise — 2025 MSP Threat Report: Threat landscape analysis and MSP security insights
- ConnectWise — Turning Prevention into Profit (2025): Proactive vs reactive service delivery models
- ScalePad — 2025 MSP Business Trends Report: Retention rates, CSAT scores, revenue benchmarks
- Pax8 — The Agentic Inflection Point (2025): MSP model maturity and strategic advisory evolution
- IBM — Cost of a Data Breach Report 2025: $4.88M average global breach cost
- Kaseya — 2025 SMB Cybersecurity Data: $140K average phishing-related SMB breach cost
- FBI — 2024 Internet Crime Report: Ransomware and phishing complaint statistics
- NinjaOne — 7 SMB Cybersecurity Statistics (2025): ConnectWise data on SMB business impact fears
- Axcient — SMB IT Security Needs Report: Service quality and provider switching triggers
- Montra Technologies — Top Reasons Companies Leave Their MSP: Post-cyberattack MSP switching data
- Verizon — 2025 Data Breach Investigations Report: Ransomware and breach trend data

Prepared for Spector.ie | February 2026 | Based on Market Sentiment Research & Industry Data