



Turn IT Costs Into Business Value

2025 IT TRENDS REPORT



When Your Budget Tightens, Strategy Matters More

This Q3 edition of our quarterly IT trends report comes at a critical moment. As IT budgets stabilize or shrink, forward-looking leaders are leveraging technology to navigate volatility, boost efficiency, and build operational resilience. In an era where trust is currency, IT decisions are no longer purely technical—they are strategic moves that shape brand trust and long-term success. The organizations that treat IT as a catalyst for change, not a cost to contain, will be the ones that adapt faster, earn deeper trust, and emerge stronger.

Unlike traditional managed service providers (MSPs), we don't just manage IT, we guide how you invest in it. "At ISOOutsource, we help businesses reframe IT from a cost center to a business-growth engine. That means focusing every dollar where it delivers the most value, such as compliance; scalable, secure infrastructure; and strategic support that drives business outcomes," says Naveen Rajkumar, CEO and President of ISOOutsource.

This Q3 2025 quarterly IT Trends update addresses top technology issues for small and midsize businesses (SMBs) with insights and advice on turning IT spend into growth leverage. To learn more about the top issues on executives' minds, read our original [2025 IT Trends Report](#), based on a survey that targeted 50,000 small and medium businesses (SMBs) across the United States. The responses revealed widespread concerns about escalating costs and underutilized technology.

Where IT Means Business: Three Routes to Business Growth in 2025



The relationship between IT strategy and business success has never been more crucial. Business leaders recognize that IT investments aligned with core business goals can reduce risk and drive long-term growth, resilience, and adaptability.

To achieve this, businesses are adopting a multi-faceted approach that emphasizes the following key areas:

- **Aligning IT with core business outcomes.** Organizations want to ensure that every IT dollar contributes directly to measurable business benefits.
- **Investing in risk management and cost reduction.** This includes not only strengthening cybersecurity frameworks but also integrating automation tools to minimize operational waste and human error.
- **Evolving IT delivery models to enhance agility.** Modern IT delivery models, such as scalable cloud solutions, hybrid infrastructures, and advanced support systems, enable businesses to maximize performance without overcommitting resources (such as investments in on-premises hardware or inflexible contracts).

IT Strategy is Business Strategy



Smart spending isn't about cutting IT. It's about aligning it with business needs. Strategic IT investments enable growth, efficiency, and resilience.

ISOutsource helps CEOs and business leaders rethink their technology investments—not just to stay running, but to stay competitive. Let us help you rightsize your IT, reduce waste and risk, and drive outcomes that matter.

With no locked-in contracts, working with us is low-risk. You can get specialty engineering to support your internal IT Team and change your support level or leave anytime.



**"It's not about tools. It's about business goals.
Start there, and the tech decisions follow."**

—Kenny Gluck, Managing Consultant, ISOutsource

Strategic Initiatives:

Restructuring IT Investment for Business Value

Leaders are auditing and reallocating IT budgets to reflect real business priorities, not outdated tools or unnecessary contracts.

It's important to know what's in your contracts, whether they're for cloud services, hardware, helpdesk support, or other IT related resources. Kenny Gluck, Managing Consultant at ISOutsource, advises going over each contract thoroughly, at least once a year. "As systems evolve, overspending slips through the cracks. We frequently discover that clients have been paying hundreds or thousands of dollars a month for legacy services they no longer use," he says.



**"Want to keep your existing IT infrastructure?
Or to spend half your budget on cybersecurity
and half on automation? We can work with that."**

—Kenny Gluck, Managing Consultant, ISOutsource

A smart approach combines regular invoice auditing with risk-based prioritization. "If someone comes to me with \$10,000 to spend, I start with where their business is most exposed—what can't they afford to lose?" says Gluck.

For SMBs especially, this approach is vital. Every company, no matter its size, has the same security threats to address, but SMBs must typically do this with a smaller budget. Underinvesting in cybersecurity is quite common for this reason, but risk-based prioritization helps CEOs know they're spending strategically. "We don't just manage IT. We help clients manage vendor contracts to align spend with actual business needs. That's where real ROI starts," says Gluck.

Balancing In-House and Outsourced Models to Rightsize IT Spend

Internal IT teams can be costly, rigid, and underused—especially for midsize businesses. As Chris Preti, Principal Consultant at ISOutsource, puts it, “With an MSP, you get scalable expertise at every level, from desktop support to consulting, on demand. To replicate that in-house, you’d need to hire at least four full-time roles, and you still wouldn’t match our coverage or redundancy.”

Even companies with enough work for a full-time engineer often benefit from MSP partnerships. Co-managed models offer cost-effective escalation support, specialized project delivery, and access to broader expertise.

For SMBs, the hybrid approach is often ideal: maintaining in-house continuity while leveraging external specialists for security, automation, compliance, and infrastructure. The co-managed approach also provides access to level 1 support and provides as-needed coverage for when internal IT staff go on vacation or leave unexpectedly.

UNDERSTANDING THE **True Value Of Outsourcing**



One experienced
System Administrator
on average costs
\$100K a year



A team of 100+ experts in
Consulting, Engineering,
and Cybersecurity



For many clients, co-managed IT is the sweet spot; it helps them retain internal knowledge while gaining access to ISOutsource’s broader team. Outsourcing gives clients exactly what they need, when they need it, with none of the overhead of an employee.”


—Chris Preti, Principal Consultant, ISOutsource



Rightsizing Through Wise Spending and Flexible Partnerships

An experienced MSP can also help businesses rightsize their investments through knowledge of the solution landscape. Kenny Gluck's approach is to examine companies' IT and business environments and then factor in costs. "Clients know what they can afford. I can offer low, mid, and high-tier options for every solution they need, taking into account their priorities and the features and performance of the possible solutions. Want to keep your existing IT infrastructure? Or to spend half your budget on cybersecurity and half on automation? We can work with that," he says.

Gluck describes a situation where flexibility was the answer to rightsizing. A client had to downsize headcount significantly, and ISOutsource helped the company adapt for the short term. "We migrated a few functions to the cloud, where it made sense, which eliminated some costs. We also moved a service to a different vendor. The original vendor does a great job, but the client was in a good position to save money by using a newer service provider that had been around for three years versus 20, which was reflected in the new vendor's lower price. We saved them roughly \$2,000 a month while maintaining same level of service and security."



There are more spending adjustments you can make now to stretch your IT dollars further. Some of these may work for you depending on your industry, business goals, and existing contracts:

- **Extend the life span of your IT equipment.** Regular hardware cleaning keeps dust out of hardware, and timely software upgrades help you take advantage of the performance improvements included in them. Ongoing health monitoring keeps you aware of things you can adjust, like temperature, power supply status, and fan speed, to extend hardware lifecycles, reducing capital expenditures and downtime.
- **Consolidate tools.** Cutting redundant software reduces licensing fees and makes systems easier to manage. You can also centralize with unified toolsets like Microsoft Teams or Cisco Webex, which has the added benefit of simplified patch deployment, compliance reporting, and staff workflows.
- **Automate common tasks.** Remote monitoring and management help keep systems running smoothly and identify potential issues so you can fix them before a problem develops. There are money-saving automations out there for finance, inventory, invoicing, marketing, project management, customer support, and many other workflows.
- **Migrate to the cloud instead of replacing expensive hardware.** By switching to cloud services, you pay only for what you use with subscriptions based on the number of people who use each service. Your company can stop paying so much to add, replace, and maintain physical storage and hardware, like hard disk drives, servers, and phone systems.
- **Defer some of your tech costs.** In addition to postponing hardware replacement costs by extending lifespans through proactive maintenance, you can prioritize replacing critical systems only. Postpone projects like website redesigns, automation initiatives, or the rollout of advanced analytics unless they directly tie to revenue or core operations.

Businesses can also rightsize their MSP support as needed. “ISOOutsource doesn’t require a locked-in contract, and SMBs can change their spend on a monthly basis. With no long-term contracts, you can pivot as your business does. ISOOutsource is an IT partner you won’t outgrow,” says Jason Lathrop, Vice President of Technology and Operations at ISOOutsource.

Important: Security isn’t something you should cut back on even in lean times. Continue to invest in:

- Cybersecurity solutions that protect your data, systems, and reputation every day.
- Vulnerability assessments to help find new weaknesses that can develop over time or in response to organizational shifts.
- Data backups and business continuity measures and security training for staff, which are always vital.
- Patch management and software updates to correct known vulnerabilities.

Incident response planning to help you determine what you’ll do in the event of a cyberattack. You’ll need to have a plan if your systems suddenly go down and attackers are demanding a ransom.

Proactive Measures:

Automation and Avoiding Sprawl

Automation has emerged as a powerful tool—but only for the right processes and companies. Implementing generative AI-based and other types of IT automation incorrectly can expose businesses to data leaks, security issues, [legal and compliance risks](#), and [process and data errors](#). It adds up to all these risks plus operational disruptions and maintenance headaches if automation is not carefully designed, secured, and monitored.

Chris Preti says, “Automation saves time only when the process is tightly defined. It’s not ‘set it and forget it’—it must be maintained. Otherwise, you just shift the workload from manual processes to fixing broken scripts.”

That said, the payoff is real in the right situation. Businesses that regularly audit and assess their IT environments, processes, and contracts can benefit when they automate repetitive, time-consuming tasks—like onboarding or offboarding users, patching systems and software, or imaging devices. Automation also [reduces human error](#).

Preti highlights a recent example of a healthy ROI: “We spent 5 hours building an automated imaging process that saved a client 20 hours of labor. That’s a 4X return almost immediately.”



“We spent 5 hours building an automated imaging process that saved a client 20 hours of labor. That’s a 4X return almost immediately.”

—Chris Preti, Principal Consultant, ISOutsource

When it comes to ROI, CEOs must weigh business priorities against their IT budgets and capabilities. Gluck says, “There is no one-size-fits-all priority, though I always advise investing in cybersecurity. Preventing a data breach with security assessments, endpoint detection and response, and other measures is always worthwhile. In this case, ROI equates to business value. It’s hard to put a price on protecting your sensitive data, your brand’s reputation, and your uptime, as they are precious.”



Tool Optimization and ROI

Tool sprawl is a big source of waste. Without a clear business case, careful product research, and regular IT environment audits, businesses can purchase overlapping or underused solutions based on hype, not need.

“You must educate yourself—or ask your MSP—to get the most value from a solution. I’ve seen products with a slick UI and great marketing, but they use the same core technology that powers tools that cost half as much. In those cases, you’re paying for the pitch, not the performance,” says Gluck.

To avoid sprawl, prioritize tools that align with real operational risks: data loss prevention (DLP), [endpoint detection and response](#) (EDR), and multifactor authentication (MFA) tools that mitigate breach costs and regulatory risk.

“Security tools don’t generate ROI in the traditional sense—but they protect it. They prevent the six-figure losses that can follow a breach. They can also prevent downtime and possible fines from compliance violations,” says Gluck. In addition to improving security, [disaster recovery](#) (DR) testing, endpoint patching, and behavioral security are also great examples of processes that can be automated.

For generative AI tools especially, Chris Preti suggests narrowing down the specific issue you want to solve. “Look at it as problem solving, not product shopping, and you can avoid tool sprawl,” he says. “Prioritize security first, then look at your budget. A good MSP can find you the right tool to solve real business issues with that formula and their knowledge of the solution landscape.” At ISOsource, we evaluate tools based on your goals, not our vendor relationships.

Protect Data and Systems Based on Risks to Your Business

Downtime has a cost, and business leaders should know what that cost is.

There are two crucial figures that CEOs must determine. While MSPs can assist by asking the right questions, only executives know their bottom line well enough to decide here.

The first figure is the Recovery Time Objective (RTO), which is the acceptable amount of downtime a business can tolerate. It's the target time for restoring a system or application after an outage or disaster. Similarly, a Recovery Point Objective (RPO) focuses on data loss. It defines the maximum amount of data loss that an organization can tolerate after a disaster or outage. These figures shouldn't be guesswork;—they must be grounded in business impact.

As an MSP helps you calculate these figures, they can also identify critical systems and specific risks around DR. to help ensure that the most vital systems are restored first and data loss is kept within acceptable limits.

Considering that [61% of small businesses were attacked in 2023](#), DR planning is essential. Data breaches and other forms of [cyberattacks cost a median \\$46,000](#) in ransomware and extortion (but more than half of the victims paid more than \$100,000). [And nearly one in five SMBs is at risk of shutting down after a cyberattack](#).

"You don't realize how much that POS system matters until it's down and you can't sell anything. Every hour counts, and every hour costs," says Preti. "In DR, your ROI is relative. If a single security event that lasts two days would cost you \$100,000, and by spending \$50,000 you could prevent that event or ensure that it would only last two hours, you're coming out ahead by \$50,000."

Disaster recovery isn't one-size-fits-all. It's a tailored investment based on operational and financial realities. "A week of downtime could shutter a small business. For some clients, we recommend shifting services to SaaS wherever possible—it reduces the need for DR platforms," adds Preti. DR plans should be tested and updated regularly as businesses add and remove systems, to make sure the data being backed up is still being used, and that all components of the plan still work.



Steps you can take toward disaster recovery today:

- **Define your business-critical systems.** Perform a business impact analysis (BIA) to determine which applications and data your business can't operate without for even a few hours. Prioritize those in your DR plan. This helps you avoid the expense of recovery systems for low-priority tools.
- **Rightsize your RTO/RPO.** Establish RTO and RPO based on business impact, not best-case ideals. For example, a law firm might need email restored within an hour, but their archived file shares can wait 24–48 hours.
- **Use the cloud for cost-effective backup & failover.** Cloud-based DR and backup solutions offer scalable, pay-as-you-go pricing, which is normally more economical than maintaining an on-premises DR infrastructure. Keep in mind that cloud DR is subject to bandwidth and networking capabilities, while your on-premises DR could be damaged by a natural disaster.
- **Test your recovery plan at least once or twice a year.** Testing is the only way to ensure that your DR plan works correctly. Schedule at least one full DR test per year, and also after any major infrastructure, hardware, organizational, business-process, or software change. Rapidly growing organizations and companies in highly regulated industries may need to test more often. This includes training your staff on response procedures and who does what during an outage.
- **Bundle DR into your broader security spend.** If you're already investing in managed detection and response, endpoint security, or cloud services—many of those platforms include DR capabilities. Use what you already have.
- **Use co-managed IT for DR planning.** If your internal team lacks time or expertise, work with an MSP to co-develop and maintain your DR strategy. This avoids the cost of hiring full-time staff while ensuring resilience.
- **Understand SLAs with your vendors.** If your business relies on cloud or SaaS vendors (Microsoft 365, Salesforce), there may be built-in features for data protection and service availability. Before you rely on these, sure you understand the scope and time frame of data you can recover from these services.
- **Don't over-invest in low-risk areas.** Avoid the temptation to build a "perfect" recovery plan for every system. Prioritize the most critical data and decide how often to update those backups according to how quickly your data changes and the cost structure of your service (more frequent backups can cost more).

Efficiency Looks Different by Industry— Here's How to Get It Right

Smart IT spending starts with understanding what efficiency means in your sector. Across industries, the goal is the same: reduce risk and overhead while protecting what matters most. How that looks in practice varies depending on regulatory, operational, and cultural factors. Here's how we help clients tailor their approach.

Manufacturing: Protect legacy equipment via segmentation and perimeter controls. Legacy systems often run mission-critical processes, but they weren't built with modern cybersecurity in mind. Rather than rip and replace, manufacturers can safeguard production environments through [network segmentation](#), strict perimeter controls, and role-based access. This limits exposure while maintaining uptime.

"In manufacturing, it's not about modernizing everything overnight—it's about protecting what keeps the line running," says Preti.

Healthcare: The most effective organizations combine staff training with layered technical safeguards like endpoint detection, encrypted communications, and routine access audits to stay aligned with HIPAA standards. Keeping policies and procedures clear and current and accessible is vital for reducing risk and protecting patients and staff.

"A smart security strategy trains people and technology to work together helps prevent mistakes, data breaches, and possible fines," says Gluck.

Legal: DLP is an affordable strategy for client data protection. Law firms handle huge amounts of client data, most of which is highly sensitive. Many are embracing DLP policies as a cost-effective way to reduce exposure without disrupting operations.

Properly scoped, DLP tools can flag risky behavior before it leads to a breach.

Preti says, "For the legal industry, it's not about locking everything down—it's about knowing where the risk lives and putting the right controls there."

Construction/AEC: Enabling secure, efficient collaboration is essential. Outdated or siloed tools and systems can create friction between field and office teams by slowing collaboration. Cloud-based solutions, combined with secure file sharing, access controls, and endpoint management, enable mobile teams to work efficiently without compromising security or budget.

"When job sites are remote and teams are dispersed, the right tools make all the difference—but they need to be secure and scalable," comments Gluck.

Nonprofit: Focus on the highest-ROI security layers; reduce overhead through automation. Every dollar matters in the nonprofit world. That's why the focus should be on high-impact, low-overhead solutions, like automation for patching and user management, or bundling core security services.



"We help clients swap tools without losing protection. One nonprofit client saved \$2,000/month by switching vendors—same functionality, lower cost." says Kenny Gluck.

To conclude, it's helpful to **work with an MSP who knows your industry**, because they already understand your compliance requirements, threat landscape, and critical systems. They can implement the right security controls from day one, without learning through trial and error. You get:

- **Faster problem resolutions.**
- **Better protection against industry-specific threats.**
- **Technology decisions that support your business operations without costly disruptions.**

Working with ISOsource has the added benefit of offering sector-specific expertise without locking you into a one-size-fits-all model. There are no locked-in contracts or standard solutions that don't fit your needs.



Let's Turn IT Spend Into **Business Value**

ISOsource helps small and midsize businesses make smarter, more strategic IT decisions that improve outcomes, not just operations.

Whether your goal is to:

- **Cut waste** by eliminating unused tools or contracts
- **Rightsize your support model** with flexible, fully outsourced IT
- **Boost ROI** through automation and smarter resourcing
- **Protect what matters most** with proactive cybersecurity and disaster recovery
- **Align IT strategy** with business growth and compliance goals

We'll help you simplify, save, and protect your business, backed by a business-first partnership model you won't find with a typical MSP.

No locked-in contracts. Just results.

Let's discuss how your IT strategy can drive real business outcomes.

Contact ISOsource today.

www.ISOsource.com