The Logical Advantage

TeamLogicIT®
Your Technology Advisor

NOVEMBER 2025

Co-Managed IT Enables AI Adoption

CIO magazine's recent "State of the CIO" study shows the top task enterprise CEOs have for technology leaders in their companies is implementing **artificial intelligence (AI)**.

Why should leaders of small- to medium-sized businesses (SMBs) care about the strategic agenda of big corporations? Because today, integrating AI into the **digital transformation (DX)** of business operations is becoming an inescapable competitive requirement across the spectrum of organizations. And because DX can provide an edge to SMBs without access to the depth of funding and technological resources available to competitors operating at enterprise scale.

Adding AI into technology infrastructure can be vexing for senior management at SMBs because they rarely have the headcount or funding for a full-time executive like a CIO. That's why we recommend co-managed IT. While you tackle trending strategic challenges, we align the core technologies of a modern, optimal, innovative tech infrastructure in these areas:

- A **scalable, flexible cloud services**
- A **secure, resilient network**
- A progressive **AI development plan**

Our transformation knowledge comes from working for an array of clients operating in diverse industries. Our services provide:

- **Technical Skills** – Expertise in multiple platforms with local onsite assistance
- **Technical Support** – Ready to assist 24/7 year round
- **Technical Nexus** – A Network Operations Center (NOC) with 24/7 remote monitoring systems
- **Technology/Business Review** – Insight grounded in performance metrics

Call us for a consultation.

The Logical Advantage

Viewpoint

vCIO Services Streamline AI Integration

Workforce studies suggest that corporate employees are adopting **artificial intelligence (AI)** technologies faster than internal IT teams can vet these applications per imperative considerations such as cybersecurity.

Meanwhile, three in five workers polled in a recent survey reported that they are using unsanctioned AI tools more than they were last year, giving rise to what some tech analysts have dubbed "**Shadow AI**." The term is a reference to the established concept, Shadow IT, when team members procure and use devices and/or software without their IT department's knowledge and permission.

Given these facts, it's not surprising that nearly two-thirds of enterprise tech leaders consider data exposure the primary risks surrounding shadow AI.

Why should executives at small- to medium-sized businesses (SMBs) pay attention to how their counterparts at big companies grapple with issues like integrating AI into their operations? Because SMBs share objectives with large enterprises, namely:

- **Driving growth** in revenue and innovation through digital operations
- **Improving digital experiences** for customers, employees and partners
- **Scaling productivity** through managing the expenses of digital systems
- **Improving the quality** of products and services delivered digitally

That's why we are supported by virtual CIO services (vCIO) that **streamline digital workflow** for greater productivity and risk mitigation: technology roadmaps, planning and budgeting and risk assessments.

How can your organization take advantage of vCIO services? Call us for a consultation.

IT Strategy

BUDR Services Mitigate Ransomware Risks

Analysis shows that ransomware levels can vary quarter to quarter. But over the long run they keep on climbing.

For example, studies earlier this year found that ransomware attacks declined more than 20% from Q1-2025 to Q2-2025. The same research, however, also discovered that incidents of ransomware rose about two times when compared to the same period in 2024. A similar study revealed that the number of active ransomware groups grew 45% from 2024 to 2025. Meanwhile, the average cost of recovering from ransomware occurrences ballooned to exceed $4 million.

True, this multimillion-dollar statistical mean largely reflects the financial risks of cybersecurity breaches facing large enterprises. But these stats also underscore the fact that a successful ransomware assault could substantially damage an organization of any size, especially small- to medium-sized businesses without the figurative deep pockets of their corporate counterparts.

That's why we advocate implementing comprehensive **backup and disaster recovery (BUDR)** systems. A full BUDR routine keeps your company's data safe, intact and recoverable by:

- Maintaining regular **local image backups** of operating systems, applications and databases.
- Generating and storing **off-site backups** daily as protection against disruptions and breaches.
- Sustaining this **hybrid configuration** rapid restoration in the wake of cyber disasters like a ransomware incursion.

We have proven BUDR policies, practices and protections to share. Call us to support your business continuity planning (BCP).

Visit our blog for more trending technology articles at TeamLogicIT.com/blog.

ITinflections NAVIGATING TECHNOLOGY FOR BUSINESS®

20 YEARS TeamLogicIT® Your Technology Advisor