The Logical Advantage

TeamLogicIT®
Your Technology Advisor

JUNE 2026

How MSPs Accelerate AI Adoption

Research by the Global Technology Industry Association (GTIA) confirms that adopting **artificial intelligence (AI)** technologies is not solely an imperative for large enterprises. Nor is the focus of AI initiatives limited to **generative** and **agentic AI** tools. Per GTIA's "Building AI Strategy" report, organizations are working to incorporate AI applications into their **digital business transformation (DBX)** efforts. Among shared priorities across industries are:

- Automation
- Data analysis
- Cybersecurity
- Software development

Why should leaders of small- to medium-sized businesses (SMBs) scrutinize this list? Because GTIA's studies verify that SMBs are a driving force in the nation's economy. Per Small Business Administration (SBA) statistics:

- SMBs have created 17 million jobs during the last 30 years.
- SMB-generated employment represents close to half the country's private sector payroll.

And AI can help SMBs sharpen their competitive edge across the spectrum of competitors, small and large. How can TeamLogic IT support SMBs pursuing AI adoption?

- Building **cyber resilience** by facilitating Zero Trust security
- Empowering **mobile productivity** for remote workers
- Enabling **business continuity** for robust backup and disaster recovery (BUDR) routines

Seeking to amplify your IT with AI? Call us for a consultation.

The Logical Advantage

Viewpoint

MSPs Strengthen SMB Cyber Resilience

Cyber-enabled fraud represented more than 80% of all losses reported to the FBI's Internet Crime Complaint Center (IC3) in recent years. Per studies by McKinsey and other analysts, one force driving this crime wave is cyber crooks increasingly using **generative AI** tools to innovate multichannel phishing techniques:

- SMS (smishing)
- Voice messaging (vishing)
- QR Codes (quishing)

This surge in cybercrime has fueled a 1,200% increase in phishing attacks in recent years and doubled average ransomware payouts in the past year.

This mega-trend is not limited to large enterprises. In fact, research also confirms that cyber fraud disproportionately affects our nation's 33 million small- to medium-sized businesses (SMBs) because many lack the deep pockets and operational resources of their corporate cohort.

How do managed services providers (MSPs) fortify **cyber resilience** for SMBs confronting today's cybersecurity risks? By helping them apply **"Zero Trust"** practices:

- Monitoring network traffic for cyber threats continuously
- Adjusting, refining cybersecurity policies, protocols and procedures continually

Our approach to managed IT services includes:

- **Proactive IT** — Flexibility, scalability for meeting new challenges
- **Preventative IT** — Anticipating, avoiding operational disruptions
- **Responsive IT** — Skilled technicians, responding onsite and remotely

IT Strategy

Training Repels AI-Enabled Ransomware

Per a recent Microsoft study, AI-generated "phishing lures" are 4x more effective than bait designed by humans without AI assistance.

A "lure" is the forged content leading social engineering campaigns that entice individuals within an organization to offer confidential credentials or click links that download malicious programming like ransomware. And plentiful research confirms that phishing remains the preferred attack vector for cyber criminals engaged in the ransomware business.

In fact, the FBI reports that a growing percentage of the millions of instances of cyber fraud they track involve "deepfakes" – i.e., scams including images, videos or audio recordings altered by **generative AI** apps.

Deepfakes have become extremely lucrative tactics for extortion techniques like ransomware, as cyber crooks use AI to impersonate executives and other business managers with the power to authorize network access and financial transactions.

As a premier **IT managed services provider (MSP)**, TeamLogic IT advocates training as the best defense:

- **Set Up Simulations** – Show staff how cyber thieves operate using real-world examples of AI-generated lures
- **Rev Up Reminders** – Increase the frequency of notices of when it's time to update passwords and other credentials
- **Workshop It** – Offer cybersecurity education options in person and online as ways to implement the first two methods

Want support running your cybersecurity training program? Give us a call.

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

ITinflections NAVIGATING TECHNOLOGY FOR BUSINESS®

TeamLogicIT® Your Technology Advisor