The Logical Advantage

TeamLogicIT®
Your Technology Advisor


# Where Leadership Shapes AI Success

During the first quarter of 2026, executives at corporations listed on the S&P 500 spoke the term "AI" during earnings calls nearly 5,000 times. An obvious sign of how pervasive **artificial intelligence** has become in U.S. business culture.

Why should this trend matter to executives leading small- to medium-sized businesses (SMBs)? Here are three reasons:

1. SMB-generated employment represents close to half the country's private sector payroll.
2. Studies show as much as half of all SMB workers already use AI apps on the job.
3. Technologies like AI enable SMBs to compete with larger companies at unprecedented scale.

In short, fostering a culture that fosters AI adoption can sharpen an SMB's competitive edge. That's why we offer these leadership tips to our clients:

1. **Lead by Example** – Culture flows from the top. Set the tone by starting conversations about AI within your team.
2. **Put Policy First** – Develop and establish formalized policies and guidelines specifically for working with AI platforms.
3. **Experiment Responsibly** – Identify where prime opportunity lies. Then, deploy frameworks and implement controls that amplify these opportunities.
4. **Share Knowledge** – Educate and train your employees internally or through online courses.
5. **Train, and Train Again** – Educate employees at all levels – from frontlines to C-suite.

Intrigued by AI opportunities? We can help you realize them. Call us for a consultation.

The Logical Advantage

# Viewpoint

## How SMB Execs Can Lead AI Transformations

Research reveals that eight in 10 C-suite leaders expect the level of change driven by digital business transformation (DX) to rise steadily during the next year. Still, more than half of those same execs feel unprepared for this intensity of technological disruption, which is largely fueled by integrating **artificial intelligence (AI)** tools into business operations.

What do these findings have to do with small- to medium-sized businesses (SMBs)? Other studies show the pace of AI adoption accelerating among SMBs, with implementations jumping by as much as 40% year to year. Why should SMB leaders embrace this movement? Because SMBs share these DX objectives with their corporate counterparts:

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

And because AI-powered DX can provide SMBs with a competitive edge versus companies operating at enterprise scale with greater funding and technological resources.

But as SMBs rarely have headcount for a full-time executive like a CIO, incorporating AI can be vexing for their management teams. That's why our national team supports us with **virtual chief information officer (vCIO)** services that we can engage locally on your behalf:

- Technology roadmaps
- Planning and budgeting
- Risk assessments

Call TeamLogic IT to learn more.

# IT Strategy

## Mitigating "Insider" Threats in SMBs

Recent studies show an increase in the number of so-called "insider" cybersecurity incidents during the last year at an estimated cost per occurrence rising above $13 million – an operating risk that can threaten the livelihood of small- to medium-sized businesses (SMBs).

A user working within the boundaries of a company's proprietary network – e.g., employee, contractor, business partner – is considered an "insider."

According to Forrester Research, about a quarter of all data breaches over the last 12 months resulted from internal events. But while greater than 40% could be characterized as spurred by deliberate negligence or malicious intent, a third sprung from accidents or inadvertent misuse.

Analysts expect this escalating trend to continue into next year. Which is why we recommend that SMBs take heed and engage **24/7 endpoint and identity monitoring** services as a defense:

- **Endpoint Monitoring** – Our Security Operations Center (SOC) watches network endpoints (e.g., desktops, laptops, smartphones, tablets) for suspicious activity. Confirmed threats launch a series of actions that immediately address the issue, prepping for eventual remediation.
- **Identity Monitoring** – Our SOC team examines sign-ins and other authentication processes across applications and cloud services to detect unusual behaviors and patterns that signal trouble. Countermeasures may include isolating an identity, forcing sign-out or freezing an account.

Continuous monitoring helps SMBs stop insider threats before damage occurs.

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

ITinflections NAVIGATING TECHNOLOGY FOR BUSINESS®

TeamLogicIT® Your Technology Advisor