The Logical Advantage

TeamLogicIT®
Your Technology Advisor

OCTOBER 2025

"Tipping" Toward Cyber Resilience

Seven of 10 technology leaders polled by the World Economic Forum (WEF) believe small- to medium-sized businesses (SMBs) have reached a "cybersecurity tipping point" where they may not be able to effectively secure their organizations against the increasing "complexity of cyber risks."

What's more is a third of SMBs told WEF researchers they already feel their **cyber resilience** is inadequate, a proportion that has swelled sevenfold in the last three years.

What are the drivers of this mass anxiety among SMBs? Artificial intelligence (AI) is one.

Why? Because cybercriminals armed with **AI-powered automation** can attack thousands of SMBs at once, exploiting companies with weak fortifications that lack dedicated security teams working with their own advanced AI tech.

That's one reason CISA, the federal agency charged with cyber defense, in collaboration with the private sector National Cybersecurity Alliance, designates every October **Cybersecurity Awareness Month** to bolster vigilance across the business spectrum.

That's also one reason our parent organization named a virtual chief artificial intelligence officer earlier this year.

Among this visionary executive's missions is providing our national network of premier managed services providers (MSPs) with insights, strategies and tactics into countering AI-generated cyber assaults with AI-fortified defenses. In fact, we already have a white paper about it.

Interested in learning more about how we can apply AI tools to your cyber defenses? Call us for a consultation.

The Logical Advantage

Viewpoint

A 2026 IT Budget Planning Primer

Gartner predicts small- to medium-sized businesses (SMBs) will increase their IT spending next year by about 10%. How will SMBs invest this technology funding? Three critical areas:

- **Digital Transformation (DX)** – Studies verify that more than half of our nation's 33 million SMBs actively are pursuing DX despite budget constraints.
- **Cyber Resilience** – Cyber resilient companies anticipate, endure and recover from digital crises like ransomware attacks. Considering that a single breach can generate remediation costs in the millions, this risk management investment yields obvious returns.
- **Competitive Advantage** – As demand for artificial intelligence (AI) tools rises, SMBs compete with each other and large corporations in the race to put these applications to work for customers, employees and partners. Furthermore, SMBs face intensifying competition among each other and big companies in the hunt regionally and nationally for technical talent that can integrate these platforms into IT infrastructure.

How do managed services providers support SMB executives with these imperatives? With three vital tech operations:

- **Cloud Computing** – Solutions delivered using an "as a service" model, with smaller periodic payments (i.e., monthly, annually).
- **Cybersecurity Programs** – Routines that continuously assess the threat landscape, monitor and maintain preventative measures.
- **Network Operations** – A local team of technicians skilled in the latest techniques responds to your needs, both onsite and remotely.

Not sure what to include in your 2026 IT budget? Give us a call.

IT Strategy

Cyber Resilience Takes More Than Tech

Studies show one in five small- to medium-sized businesses (SMBs) have filed for bankruptcy or permanently ceased operations after just one data breach.

Why? Because research also reveals that for more than half of SMBs a financial loss of $50,000 or less could force them out of business. Which is what makes common **cyber attack techniques** such as ransomware—when cybercriminals penetrate company networks, take over servers and encrypt vital operating data—potentially devastating for smaller companies.

To return access and control, perpetrators demand firms pay ransoms in the form of cryptocurrencies. Analysts estimate ransomware payments topped $1 billion last year. How can SMBs avoid becoming one of the business casualties contributing to that massive cybercrime statistic?

Availing themselves of **IT managed services** powered by the latest AI-enabled cybersecurity tools is part of the answer. But the latest security technology alone is not enough. Cybersecure tech requires good systems grounded in sound policy and disciplined practices.

That's why we believe establishing and sustaining cyber-resilient operations requires a computing culture of monitoring and maintenance that expects people, not programming, to make the critical difference. And that's the reason a **chief AI officer** supports our team as we support yours.

We espouse three core principles:

- **Proactive IT**
- **Preventative IT**
- **Responsive IT**

Give us a call to discuss putting them to work in your organization.

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

ITinflections NAVIGATING TECHNOLOGY FOR BUSINESS®

20 YEARS TeamLogicIT® Your Technology Advisor