

OCTOBER 2026



Curb Cyber Risks with Co-Managed IT

Studies continually show the rising tide of cybersecurity threats shows no signs of subsiding:

- **Ransomware Remains Rolling** — Research shows the rate of confirmed ransomware attacks consistently has run higher than 1,400 annually for the last several years, despite many successful short-term countermeasures deployed by companies and government agencies.
- **Phishing Fortifies Footings** — Research shows today's array of phishing techniques continues as a foundational cyber risk, now responsible for a third of all cyber incidents, and establishing this as the top cause of data breaches.

Why should leaders of small- to medium-sized businesses (SMBs) take heed of these facts? Two reasons:

- Small Business Administration (SBA) surveys reveal nine of 10 U.S. companies qualify as “small” businesses.

- Analysts have confirmed that nearly half of all cyber assaults target SMBs.

How can SMBs stay afloat on these risky cyber waters? By implementing a comprehensive **co-managed IT services** program based on these three principles:

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

TeamLogic IT helps secure your business by collaboratively monitoring and managing your entire technology environment. Our expert support helps decrease disruptions and control costs, enabling operational efficiencies and, in turn, fostering growth.

Viewpoint

3 Pillars of Cybersecure Culture

Research reveals that **business e-mail compromise (BEC)** techniques like phishing accounted for more than \$8 billion in losses from data breaches to companies across the industry spectrum during the first quarter of 2026 alone.

Now, consider studies that indicate a financial loss of \$50,000 or less could force more than half of our nation's millions of small- to medium-sized businesses (SMBs) to close their doors at least temporarily, and the necessity for cyber resilient organizations in the U.S. economy becomes clear. That's one reason CISA, the federal agency charged with cyber defense, in collaboration with the private-sector National Cybersecurity Alliance and supported by the National Institute of Standards and Technology (NIST) and Department of Homeland Security (DHS), designates every October **Cybersecurity Awareness Month**.

As champions of managing IT to develop thriving businesses — especially SMBs — we wholly endorse this annual initiative.

What is the key to **cyber resilience**? We believe it's fostering a **cybersecure** company culture built upon three pillars:

1. **Leading by Example** — Culture flows from the top. Set the tone by starting conversations about cybersecurity within your team.
2. **Prioritizing Policy** — Develop, establish and maintain formalized policies and guidelines specifically for relentless cybersecurity.
3. **Share Knowledge via Recurring Training** — Educate and train employees at all levels, from frontlines to C suite, internally or through online courses.

IT Strategy

Essential Cybersecurity Practices for SMBs

The most important cybersecurity practices for small- to medium-sized businesses (SMBs) are employee training, strong passwords, multifactor authentication (MFA) and timely software updates. As cybercrooks deploy agentic and generative artificial intelligence (AI) to multiply illicit campaigns and diversify malicious techniques, SMB leaders are responding by increasing cybersecurity investments. Studies show:

- More than half of SMBs surveyed rank **cybersecurity** as a top priority for next year.
- Six in 10 of those companies plan to increase cybersecurity spending during the next 12 months, emphasizing AI-related security tools.

Where are SMBs investing these funds?

- **Tactical Training** — Educational courses go beyond awareness to teach employees how to recognize, report and rebuff social engineering techniques like phishing, one of the most common attack vectors against SMBs.
- **Powerful Passwords** — Training includes best practices for creating, managing and updating automation-resistant passwords.
- **Mandatory MFA** — Also called two-factor authentication, makes accounts significantly more secure, especially against phishing.
- **Unrelenting Updates** — Promptly installing software security updates eliminates major vulnerabilities.

What supporting roles do we play as a premier **managed IT services** provider (MSP)?

1. **Exhaustive vigilance** that increases early detection of cyber incursions.
2. **Rapid response** that reduces the operational risks of downtime.
3. **Proof of protection** that facilitates compliance with regulators and cyber insurance providers.

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