The Logical Advantage

TeamLogicIT®
Your Technology Advisor

JANUARY 2025

Fortify Remote Workers Against BEC

Gartner predicts companies across the board will spend more than twice as much on devices in 2025 than they will on data centers. Replacing laptops, mobile phones, tablets and other hardware purchased during the remote work era of the last several years mostly will drive this spending curve, analysts say.

This buying coincides with another expanding movement: Growth in "independent work" such as freelancing and consulting. Studies show more than 72 million people perform independent work, with nearly 30 million of them doing so full time.

Why should you, as a leader of a small to medium-sized business (SMB), heed these trends?

Because increases in the number and capabilities of devices among workers supporting your business inside or outside your formal organization directly correlates to cybersecurity risks – i.e., business email compromise (BEC), the category covering social engineering tricks that lead to cybercrimes like ransomware.

How can you manage the rising risk of BEC?

We advocate performing a thorough IT assessment aimed at delivering the highest levels of availability and security to your team members wherever and whenever they choose to work. Here are three steps:

- **Audit** all endpoints – from servers and desktops to laptops and smartphones
- **Map** your organization's virtual perimeter, considering all systems within your network's reach
- **Adopt** virtualization and cloud computing tools and techniques

We specialize in this process. Give us a call to get started.

The Logical Advantage

Viewpoint

2 Focal Points for Rapid Returns from AI

Forrester researchers predict investment in artificial intelligence (AI) will triple by 2030 at a compound annual growth rate of 36%. Applications for this rapidly emerging technology are multiplying exponentially as companies around the globe integrate innovative solutions across all phases of business, from frontlines to executive suites.

While tech newsfeeds may give the impression that only the largest organizations have the resources to ride this cresting wave, AI's very nature – i.e., a way of augmenting user experiences and increasing operator efficiencies – means this tech tool affords small to medium-sized businesses (SMBs) proportional opportunity.

AI allows SMBs to derive as much potential value and competitive advantage from IT investments as their larger counterparts.

But where should SMB leaders look to invest in AI for the most immediate, greatest returns?

- **Automation** – Routine tasks enhanced with AI-free workers to focus on higher-value activities by enabling faster turnaround times, eliminating wasted effort, heightening information accuracy and lessening errors.
- **Decision Support** – AI's ability to collect, compile, analyze and articulate information from a multitude of sources inside and outside your organization at unprecedented speeds renders tremendous insights for planning and executing all manner of business initiatives.

How could AI solutions play out at your company? Our white paper has examples in pivotal functions from customer service to financial analysis. Call us to discuss.

IT Strategy

Resist Rising Deepfakes with BUDR

Deepfakes are AI-assisted social engineering techniques that use realistic, but faked, voice calls, video clips, and live videoconferencing calls and are growing more common as a means of enabling cybercrimes.

In a recent Deloitte survey, 15% of corporate executives reported that deepfakers had targeted their firm's confidential data at least once in the last 12 months. Another 11% said their organizations weathered multiple deepfakes during the same period.

Why is this trend a growing problem for companies of all types and sizes? Because of the financial damage caused by cyber disruptions like ransomware. The costs of recovering from a single attack can run into millions of dollars when considering operational downtime that leads to losing revenue.

What's worse? Some remediating expenditures can be ineffective. Research suggests that as much as three quarters of companies that pay ransoms do not recover the stolen data.

We strongly advise implementing comprehensive backup and disaster recovery (BUDR) systems. A full BUDR routine keeps your company's information safe, intact and recoverable by:

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

Contact 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