The Logical Advantage

TeamLogicIT®
Your Technology Advisor

Lead Cybersecurity from the Top

Cybersecurity attacks inexorably are moving from risk to certainty, as cybercriminals continue to escalate and innovate their attacks.

Consider these facts from researchers at the Identity Defined Security Alliance (IDSA):

- 9 in 10 organizations experienced at least one breach within the last year.
- 7 in 10 organizations suffered direct business impact from an incursion.

These impacts presumably were negative, such as:

- Operational disruptions
- Revenue losses
- Damages to reputation

How can leaders of small to medium-sized businesses insulate their organizations from continually diversifying cybersecurity threats? In short, by leading these three initiatives:

1. Champion Policy – Lead as the driver behind four foundational policies that cover the cybersecurity spectrum from diligent preemption to best practices: Acceptable Use (of company devices), Password Protection, Breach Response and Disaster Recovery.

2. Advocate for Education – Multiple studies confirm that more than 80% of breaches involve some form of human error, such as weak password practices or a lack of awareness of prevalent social engineering techniques. Lead by provisioning funding for cybersecurity education campaigns and being an avid participant in those programs.

3. Invest in Expertise – While cultivating a cybersecure business culture within an organization is crucial, technical expertise is critical, too. Lead by expanding cybersecurity acumen beyond the boundaries of your company by engaging a premier IT Managed Services Provider (MSP.)

The Logical Advantage

Viewpoint

3 Signs It's Time to Boost IT Services

IT services have become the top business expense in history, a trend that analyst firm Gartner says runs across all industries and types of organizations worldwide from small to large.

Why? Because of the pressing practical requirements of operating and maintaining digital devices, networks and their programming around the clock, analysts say.

Concerned that your business isn't keeping pace with this global trend? Here are three signs that you may be right:

- **Cyberattacks against your company recently spiked** – Ransomware assaults broke records in 2023 with the number of victims rising 128% compared to 2022. Moreover, researchers affirm that the U.S. is the most targeted nation in the world for cybercrime.
- **Your Business Continuity routines are incomplete, inconsistent or inscrutable** – When was the last time your firm's data backup and disaster recovery (BUDR) policies, plans and processes were reviewed and tested? And if you're not sure, why trust them?
- **As hybrid working expands, your team's productivity shrinks** – Studies show three-quarters of U.S. companies reported implementing and/or expanding hybrid working models in the last year using digital tech such as collaboration tools – as nearly half of workers surveyed say they prefer part-time remote to full-time in-office work.

We have the scope of expertise and scale of service to take your IT support to the next level – whether around town or across the nation.

Ready to get started? Give us a call.

IT Strategy

Prepare Today for Tomorrow's Metaverse

Should your business plan to participate in the metaverse?

These statistics may help answer that question:

- Tech analysis firm Gartner forecasts a quarter of the world's population will spend at least an hour in the metaverse by 2026.
- Those same Gartner studies predict a third of all businesses will have products and services ready for the metaverse by that same year.
- Business consultants at McKinsey foresee that more than half of live events will be held in the metaverse by the end of this decade, a trend that could impact 80% of global commerce.

What is the metaverse?

In conceptual terms, it's a convergence of physical and digital realms resulting in a 3D virtual space where digital identities work, shop and socialize using avatars. They can move from one experience to another in real time using real currencies for commerce.

Technologically, it's an evolving business ecosystem of virtual reality (VR), augmented reality (AR) and artificial intelligence (AI).

Why prep now? Because along with huge growth potential, the metaverse represents escalating digital risk – offering cybercrooks new platforms for stealing data and perpetuating fraud.

Here's a 3-step plan that lays crucial groundwork:

1. Create a clear, comprehensive cybersecurity policy.
2. Emphasize systems monitoring and maintenance.
3. Launch a core program strictly managing devices, closely controlling network access and regularly patching software.

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

ITinflections NAVIGATING TECHNOLOGY FOR BUSINESS®

TeamLogicIT® Your Technology Advisor