The Logical Advantage

TeamLogicIT®
Your Technology Advisor

MARCH 2024

Technology Trends

Facilitate Productive Hybrid Meetings

Recent studies by Gartner concluded that hybrid meetings—i.e., some participants in the office, some attending remotely—usually are significantly less productive than in-person sessions or entirely virtual ones.

The reason, as one Forbes columnist put the matter: "When people are not equal participants in meetings, productivity suffers."

What factors could make meeting attendees "not equal?" Here are a few:

- Poor internet connectivity
- Narrow network bandwidth
- Outmoded cameras, microphones and speakers and/or drivers in desktop and/or mobile devices

In other words, less-than-optimal IT can lessen the productivity of hybrid meetings.

As a premier managed IT services provider (MSP), we can help you address the challenges listed above by:

1. Assessing current connectivity to determine any deficits

2. Testing existing systems to evaluate capacity

3. Developing an affordable transition plan for raising the performance of mobile devices and collaborative software tools

Our service objective: The highest levels of systems availability and security at any time, from anywhere—on premises or in the field.

Your ultimate solution will mix and optimize laptops, desktops, smartphones, servers, virtualization and cloud computing. Building it takes time. And keeping it solid as a foundation of productivity requires continuing care. We know how to do both.

Give us a call to get started.

The Logical Advantage

Viewpoint

Backup & Recovery (BUDR) Builds Confidence

Studies show about eight in 10 small to medium-sized business (SMB) leaders are nervous about the security of their company's sensitive information. And for good reason. One in four SMBs polled report suffering a breach in recent years.

Instances of data breaches continue to trend toward all-time highs, with breach costs—e.g., regulatory fines, legal fees, losing customers—rising alongside these escalating attacks. Losing critical data could mean losing millions, a financial impact that can cripple or extinguish an SMB.

How can SMB leaders assuage their anxiety? Establish a data backup and disaster recovery (BUDR) routine that launches in the wake of a breach or other types of data disasters.

Here are the steps:

1. Assess Loss/Damage—Was one device breached? Or many? Was the entire network compromised? Are all servers/workstations still functional?

2. Set Recovery Goals—Prioritize the most essential files. Identify the last day and time this information was intact, which is called a recovery point. Determine how long your systems require for complete restoration.

3. Select Recovery Source—We recommend maintaining three options:

- ***Local Image Backup***—Regular, ongoing backup of operating system, apps and databases
- ***Offsite Backup***—From nightly file backup to cloud-server virtualization
- ***Hybrid Services***—Combo of first two that accelerates restoration without local access

4. Confirm Recovery/Functionality—Test network connectivity and user accessibility.

5. Self-Assess Afterwards—Review, refine your process.

We have walked dozens of clients through this process. Call us for a consultation.

IT Strategy

Tighten Password Practices with Training

Research reveals many leaders of small to medium-sized businesses (SMBs) do not trust their employees to secure critical and confidential information. Why? Because analysis of data breaches indicates more than half of those incursions involve human error.

But study after study also confirms that one of the best ways for SMB leaders to address this issue is user education. And what should companies prioritize in cybersecurity training? Password practices.

The reason for that is a small change to password protocols goes a long way.

Consider these results generated from studies in IT labs... If a gang of hackers typically has the computing power to make 100 billion attempts at guessing a single employee password, then:

- A short password of six random lowercase letters could crack in a fraction of a second
- Nearly doubling the length to 11 random lowercase letters increases task time to 11 hours
- Adding random uppercase letters to the mix rockets the job to 30 months
- Sprinkle in numbers and special characters? The assignment leaps to 500 years

That's why crafting a sound password protection policy and training staff to follow it can make a big difference in reducing risk in relatively short order.

Moreover, all types of cybersecurity education reinforce a culture of vigilance in your organization that strengthens your first line of defense against cybercrime—your employees. Plus, a cyber savvy workforce produces competitive advantage as your company minimizes and mitigates operational disruptions.

Need help sharpening your password policies, practices and training? Give us a call.

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

ITinflections NAVIGATING TECHNOLOGY FOR BUSINESS®

TeamLogicIT® Your Technology Advisor