The Logical Advantage

TeamLogicIT®
Your Technology Advisor

MAY 2024

Back Remote Workers with Hybrid BUDR

Is remote work becoming today's workplace standard?

Let these recent statistics from LinkedIn's Workforce Confidence Index help answer that question:

- Just 10% of U.S. job postings at the end of last year offered fully remote positions.
- Yet, those postings received nearly half of all applications, translating into remote roles receiving 5x the share of applications than other types of jobs.
- About 60% of the respondents to this same study preferred completely remote or hybrid positions to working full-time in the office.

Two conclusions from this data are clear: Remote work will continue at unprecedented rates indefinitely. And leaders who want to compete for workers in the national talent pool should at minimum prepare to support hybrid models.

Embracing these findings increases the importance of your backup and disaster recovery (BUDR) strategy.

Why? Because increasing the proportion of remote work also elevates operational cybersecurity risks.

How to cope? As a top-tier IT managed services provider, we recommend keeping your information safe, intact and recoverable by:

- Maintaining a regular **local image backup** of operating systems, applications and databases
- Generating and storing an **offsite backup** daily as protection against failures at facilities
- Sustaining this **hybrid BUDR configuration** to enable rapid restoration in the wake of a cyber disaster like a ransomware breach

We have BUDR experience and expertise accumulated from assisting clients across an array of industries. How can we apply this knowledge to your business?

The Logical Advantage

Viewpoint

Boost Productivity via Cloud Transformation

Digital Transformation (DX) remains a global priority for organizations of all types and sizes as companies increasingly use technologies to create value through products, services and experiences.

Why should leaders of small to medium-sized businesses (SMBs) follow this trend? Because analysts say the driving force behind DX is increasing workforce productivity, which creates a direct link between managing tech and running a successful business.

And we believe for SMBs that link is the cloud. It's today's best platform for operating fast and efficiently at high impact in an increasingly mobile environment. In short, working more productively.

As a premier IT managed services provider, we can help you transform your organization via the cloud by aligning your workforce strategy with your technology strategy:

1. Perform a Cloud Readiness Assessment to determine bandwidth, reliability and security.
2. Audit connectivity to ensure system and network accessibility.
3. Review company policies for cybersecurity and cloud compliance.
4. Recommend a hybrid, private and/or public cloud for the best fit.
5. Support your cloud implementation and migration processes with continuing services.

Our knowledgeable engineers and technicians can assess your organization to identify the solutions that can best raise your operational performance.

To learn more, give us a call.

IT Strategy

Align Workplace Cybersecurity for Gen Z

Recent studies suggest that Gen Z workers, not Baby Boomers, are the most vulnerable to cybercrime in the workplace. Gen Z generally is online more, using more apps and sharing more personal information in the process than other contemporary generations, tech analysts say.

Why should these dynamics matter to leaders of small to medium-sized businesses? Because of two other trends recently uncovered by researchers:

- The job-search platform Glassdoor predicts Gen Z will make up a larger portion of the U.S. workforce than Baby Boomers for the first time this year.
- The same study found that a third of Gen Zers prefer hybrid working models and as many as three-quarters of them are willing to quit over such issues.

Retaining Gen Z talent will require companies to manage increasing cyber risk. Here's our checklist for aligning cybersecurity practices with an increasingly mobile team:

1. Assess Readiness
- Audit devices
- Verify internet connections and network accessibility
- Implement collaboration tools

2. Review Policies
- Acceptable use of devices
- Levels of privilege for access
- Response to breaches

3. Establish Safeguards
- Multi-factor authentication (MFA) for devices
- Virtual Private Networks (VPNs) for access
- Continuous monitoring for incursions

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

ITinflections NAVIGATING TECHNOLOGY FOR BUSINESS®

TeamLogicIT®
Your Technology Advisor