The Logical Advantage

TeamLogicIT®
Your Technology Advisor

AUGUST 2023 ISSUE

Technology Trends

Today's Hybrid Work Requires the Cloud

U.S. Labor Department statistics show the era of the hybrid workforce is far from over. Despite rising percentages of workers returning to the office in the post-pandemic period, some segments of the nation's economy remain heavily hybrid—or fully remote.

According to *The Wall Street Journal*, federal studies indicate:

- More than 67% of companies in the information sector, which includes media and technology firms, support hybrid staff.
- The share of hybrid arrangements among organizations in the professional and business services sector, which includes law and accounting firms, is nearly half.
- Overall, the number of businesses that moved to a total remote workforce in 2022 rose slightly.

While the balance of remote vs. in-office workers will vary among businesses and industries, some level of cloud computing is now standard IT for organizations of every type and size.

But how do you know what level of cloud services is optimal for your team? To discover the best fit, we recommend a cloud assessment that considers:

- Cybersecurity measures
- Network bandwidth
- Application performance
- Data management
- Business continuity/disaster recovery procedures

A finely tuned, properly managed cloud strategy not only helps hybrid staff stay productive, but it can help keep customers satisfied, vendors connected and all your operations humming. Call us to discuss your cloud options.

Viewpoint

Retain Talent by Supporting Hybrid Work

Earlier this year, a survey of LinkedIn users by the career website Dice.com yielded some startling results highlighting the popularity of remote work in the post-pandemic age.

Dice asked: “Would you quit a 100% remote job if your company issued a return-to-office mandate?” More than 40% of respondents said “yes.” Another 45% said they would stay in their positions only if their employers offered hybrid work options.

The implication for organizations of all shapes and sizes is clear: Every business should craft a hybrid working strategy to retain its best workers, and that design should be supported by highly available, highly accessible and highly secure IT infrastructure.

What are the critical elements of IT that enable high productivity from any place at any time? We’ve identified five core components:

1. Current, comprehensive cybersecurity, mobility and business continuity/disaster recovery policies and procedures

2. An optimized network featuring a balanced combination of on-premises systems and cloud services with access to a basic application package featuring word processing, spreadsheets and presentation tools

3. An array of mobile-ready device options—laptops, tablets, smartphones—ideally backed by help desk services with some level of 24-hour service

4. Mobile access software fortified by a secure virtual private network (VPN) with multifactor authentication

5. A collaboration platform that unifies voice, data, web conferencing, instant/text messaging and chat services

Need a hand with your hybrid plan? Give us a call.

IT Strategy

Train Users to Beware ‘Scareware’

Earlier this year, the rate of ransomware spiked to the highest levels ever observed by some monitoring organizations.

One cybersecurity threat watcher reported an overall 91% jump from one month to the next. In some sectors, such as professional services and manufacturing, attacks rose more than 100%. Other industries that saw significant increases in threats were financial services, technology, healthcare and education.

Analysts have varying theories to explain this shocking swell in cybercrime. But regardless of cause, business leaders should respond to rising cyber risks with swift preventative action. And one of the best immediate responses is emphasizing user education.

Some studies suggest awareness training can lower the risk of users falling victim to socially engineered assaults like ransomware by as much as 70%. The effects are worth the effort, as a single data breach can cost an organization from tens of thousands to millions of dollars. Stopping even one incursion could translate into a huge savings.

Cybersecurity training need not be complicated to work. For example, it might involve teaching users about “scareware,” one of the oldest, most common techniques for depositing malicious software like ransomware.

Typical scareware campaigns involve emails, texts or web pop-up alerts featuring anxious language or jarring sounds. The messages exhort users to click or call immediately to download a critical update, unlock a frozen account or avoid imminent system failure.

Scareware executions vary, but the detection rule is the same: Never trust urgent messages from sources other than your IT team.

Call us if you’d like to discuss implementing essential cybersecurity practices.

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

ITinflections NAVIGATING TECHNOLOGY FOR BUSINESS®

TeamLogicIT®
Your Technology Advisor