The Logical Advantage

TeamLogicIT®
Your Technology Advisor

JUNE 2023 ISSUE

Technology Trends

Cloud Continues as a Strategic Priority

More than three-quarters of finance leaders plan to continue investing in digital technologies this year, according to research from Gartner. These analysts predict CFOs will maintain or increase IT spending regardless of inflation levels or interest rate hikes. One area where CFOs plan to concentrate spending is in cloud solutions.

Consider these additional findings about cloud trends:

- Gartner projects overall 2023 IT expenditures will grow greater than 5% globally, with the bulk of new investments going to cloud tech.
- Worldwide spending on public cloud services (e.g., Amazon Web Services, Microsoft Azure) is projected to increase by more than 20% over last year, according to Gartner.
- Research by IDC shows year-over-year spending on computing and storage infrastructure for cloud deployments up nearly 25% by the third quarter of 2022.

Why are finance executives committing so many dollars to cloud services and infrastructure? One reason is cybersecurity. Deloitte recently found that cybersecurity provides the foundation for cloud-driven digital transformation, accounting for about half of any given initiative's success.

While these findings pertain mostly to enterprise IT, small to medium-size businesses (SMBs) would be wise to take notice. SMBs make up as much as 99% of U.S. companies per government statistics, which means these organizations compete regularly with large corporations across industries and markets.

The growth in cloud migration in recent years underscores that this is a movement that's clearly being embraced by organizations of all sizes that are looking for more secure yet flexible computing solutions.

The Logical Advantage

Viewpoint

Hybrid Working Tech: Today's IT Standard

Recent research suggests remote technologies for hybrid working are now standard IT for most businesses. That's because most employees prefer flexible policies that enable remote work but also offer access to company facilities.

Future Forum polled 10,000 workers and found 67% of them preferred hybrid arrangements with physical workspace as an option. More than half (57%) of this group also reported their company's culture improved during the last two years, citing work flexibility as a primary reason.

These findings reinforce the importance of implementing cloud infrastructure as the backbone for ensuring an effective workforce environment. Not only do cloud services allow employees to operate from anywhere at any time across multiple devices, but a cloud subscription and consumption-based business model converts the capital expense of purchasing IT into an operating expense.

If you're considering a cloud migration, we advocate this three-step approach:

1. Review requirements—Cloud migrations involve many options and just as many decisions. Your process should start with a clear understanding of exactly what your business needs to serve remote workers reliably, securely and affordably.

2. Evaluate technologies—Do you want to consider public cloud, private cloud or possibly a hybrid solution?

3. Balance configuration—Hybrid clouds combine customizable services like customer-facing applications with essential services like file synching and sharing. Also, you determine what to back up on premises and off site, and how often.

Call us if you're interested in a Cloud Readiness Assessment.

IT Strategy

BEC Attacks Never End

A spike in business email compromise (BEC) occurred along with the rise in hybrid work arrangements. As more companies and employees embrace remote work arrangements, company communications may become more vulnerable to cybercriminals.

Consider this sobering statistic: Cyberattacks on business email increased more than 80% in 2022 and 175% over the last two years.

How can your business avoid contributing to these statistics? The answers are policy and people.

Minimizing the risk of email compromise starts with addressing human error, a factor that plays a role in nine of 10 data breaches.

Help your remote employees avoid becoming BEC victims by following these three steps:

1. Lay a policy foundation—At a minimum, your IT policies should include the following: Acceptable Use, Data Breach Response, Disaster Recovery Plan and Password Protection policies.

2. Launch awareness training—Employees who understand how social engineering schemes work tend to adhere more closely to security policies.

3. Put everyone on alert—From executive suite to frontline operations, every member of your organization must participate in cyberdefense.

Give us a call if you'd like support with deflecting email schemes and other cyberthreats.

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

ITinflections NAVIGATING TECHNOLOGY FOR BUSINESS®

TeamLogicIT® Your Technology Advisor