The Logical Advantage

TeamLogicIT®
Your Technology Advisor

JULY 2024

Hybrid Work Schedules Becoming Routine

A recent Cisco study gives more evidence that hybrid work schedules are becoming a standard operating procedure for businesses around the world. Regardless of variances in return-to-office mandates, some level of working virtually on a team – whether from home, a company facility or remote locations like coffee shops – is becoming routine for organizations of all types.

Here are highlights of what Cisco researchers discovered:

- Seven of 10 remote workers surveyed responded "positively" to employers who mandated at least a partial return to office work, while few companies reported losing employees over the matter.
- Another sign that working remotely is becoming routine – especially in the U.S. – is only a third of employers polled in the Americas said they require full-time attendance in the office.
- Despite these strong trends, nearly half of respondents reported they believe their office environments are not suitably equipped for hybrid work.

Employers involved in the survey identified keeping pace with collaboration technology as a drag on productivity. How can your organization lessen this drag?

We recommend a tech assessment that aims to optimize connectivity and boost productivity wherever your team works. Here are some key considerations:

- Network access policy
- High-speed Wi-Fi service
- File sharing/task management protocols
- Audio/video collaboration tools

Need to improve the technology in your remote or hybrid work environment? Call us to assist.

The Logical Advantage

Viewpoint

Co-Manage IT to Bolster Cybersecurity

CompTIA's 2024 "State of Cybersecurity" report concludes that "risk management is the driving force behind cybersecurity," and advises that trust between a business and its service providers is the keystone for effectively managing any kind of risk. That's why as an IT managed services provider, we advocate for co-managed technology services as the foundation for cybersecure operations. Here are the cornerstones:

- Remote monitoring and management of workstations and servers
- Application and operating system patch management
- Cybersecurity essentials, endpoint protection, employee security awareness training
- Business grade backup and disaster recovery (BUDR)

Build on this foundation with fundamental Help Desk services that prioritize security:

- 24/7/365 coverage
- Certified technicians with continual training
- Call tracking from initiation through resolution

Augment this IT service program with Virtual CIO Services (vCIO) that streamline workflow for risk mitigation. A vCIO supports:

- Ongoing IT planning and budgeting
- Regular infrastructure risk assessments
- Deploying updates and upgrades

Until recently, only large organizations had the financial resources for a dedicated CIO position. But escalating cybersecurity risks have made this type of management for small to medium-sized businesses a necessity. Call us to learn more.

IT Strategy

Should Your Business Go "Passwordless?"

With the rise of digital identities for individuals around the world and companies of all kinds, technology strategists increasingly advocate for "passwordless" authentication as a means of mitigating cybersecurity risks. Here's the research that supports their case:

- About nine of every 10 organizations across industries use passwords as the prime IT user authentication method.
- Yet, nearly half of all data breaches involve stolen credentials – primarily passwords.
- Meanwhile, conventional countermeasures – such as lengthening passwords – are losing potency; research shows more than 30 million breached passwords had over 16 characters, challenging the efficacy and long-range viability of longer passwords.

So, tech analysts argue the time has come to evolve fully to the next level of authentication. Often combined with two-factor authentication (2FA) common passwordless methods include:

- **Passkeys** – digital credentials stored on the user's device – e.g., biometrics like fingerprint or facial recognition
- **One-time Passcodes** – digital credentials randomly generated by a separate system then sent to a device under the user's direct control – e.g., passcodes sent by text, email or automated call from a trusted number; these codes expire typically in 10-30 minutes
- **Magic Links** – same concept as one-time passcodes

Should your business go passwordless? The answer depends on multiple factors such as your cyber risk profile, transition timetable and available budget. We can help with this analysis.

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

ITinflections NAVIGATING TECHNOLOGY FOR BUSINESS®

TeamLogicIT®
Your Technology Advisor