The Logical Advantage

TeamLogicIT®
Your Technology Advisor

SEPTEMBER 2022 ISSUE

Channel Futures
MSP 501
TWO-TIME
MSP OF THE YEAR
2020 & 2021

Technology Trends

Ransomware Continues to Rise

Ransomware remains a top attack vector for cybercriminals with incidents nearly doubling year-over-year according to a recent study.

Earlier this year, the security software firm Sophos surveyed 5,600 IT professionals at midsize organizations. Their analysts attributed dramatic ransomware growth to three key factors:

1) Ransomware-as-a-Service (RaaS) enables more amateur offenders to perpetrate these crimes.

2) Attackers have sharpened their encryption skills.

3) The number of victims paying ransoms greater than $1 million more than doubled.

Here's some of the evidence supporting their conclusions:

- 66% of IT pros reported suffering a ransomware assault last year, up from 37% in 2021.
- In 2022, bad actors successfully encrypted 65% of files during incursions, up from 54% the prior year.
- The average ransom payment last year reached $812,360, increasing five-fold from 2020.

Nine in 10 survey respondents reported that ransomware attacks hindered operations, with 86% saying the most severe assaults caused their companies to lose revenue or business and required about a month to recuperate.

The rise of cyberthreats like ransomware is a major reason why the National Institute of Standards and Technology (NIST) recognizes October as Cybersecurity Awareness Month.

NIST's overarching mission is to increase the nation's resiliency in the face of today's cybercrime onslaught. We fully endorse and support NIST's cybersecurity awareness efforts. How will your company fortify its cybersecurity this October?

Viewpoint

Why IT Should Lead the Way to Hybrid Work

Remote work is here to stay, and hybrid work is the future for most employees, according to Gallup, the national polling firm. Moreover, Gallup asserts that companies that fail to offer flexible working environments risk losing competitive advantage in terms of productivity, hiring and retention, and other factors.

Since the onset of the pandemic, Gallup has studied the experiences, needs and plans of more than 140,000 U.S. workers. One research finding is that nearly 60% of employees with remote work options prefer a hybrid arrangement—i.e., a balance of working in and out of the office.

Gallup cautions that employers ignore this preference for workplace flexibility at their own peril: "Failing to offer flexible work arrangements is a significant risk to an organization's hiring, employee engagement, performance, well-being and retention strategies."

For companies of any size, permanently shifting to some balance of hybrid work may require changes in policies, practices and, of course, technologies. That's why we recommend assigning your IT team to lead the way through this digital transformation.

Why? Here are three good reasons:

1) Positions IT staff as technology leaders, directly involving you in decisions about communication, collaboration and productivity tools.

2) Provides a test case, as your IT staff serves as an incubator for new policies, practices and solutions.

3) Accelerates adoption, as technical experts learn efficiencies before rolling services into the field.

We support your progression to hybrid work with managed IT services for secure network access anytime, anywhere—onsite, remote and in the cloud.

Want to learn more? Give us a call.

IT Strategy

Train Your Tech (and Non-Tech) Security Teams

Employee education on cybersecurity should be an imperative. But at the least it's a priority for many companies.

According to the latest "State of Cybersecurity" study by global IT advocate CompTIA, 41% of companies are making employee education a security priority. But CompTIA analysts recommend opening training to all, noting, "Today's processes require specialization in the technical workforce and security-first thinking in the overall workforce, or the process of security will break down, leaving the business exposed."

Cybercrime victimizes millions of people every year, resulting in thousands of businesses losing billions of dollars annually. Cyber crooks don't discriminate between individuals and institutions.

Neither should your company. That's why we recommend education that embraces technical and non-technical staff. Here are three training tips:

- **Train up, down and across.** Make programs available to everyone in the organization from front-line employees to C-suite occupants. They probably all use technology to some extent in their roles. Open courses to every department, with topics not only specific to technologies such as the cloud but to functional areas like HR and finance. And if non-IT team members want to explore highly technical subjects, encourage their initiative.
- **Go virtual but keep it real.** Offer online programs so that employees anywhere in the field can access training, but also provide in-person sessions at regional facilities. In this age of expanding hybrid work environments, workers should have the option of attending in or out of the office.
- **Create hybrid teaching teams.** Pair technical instructors with business coaches for a complete learning experience.