



## Adopt “Cloud First” Transformation

Research reveals this year eight in 10 organizations plan to become “cloud first” enterprises at some level or make meaningful progress toward that goal.

What is a cloud-first company? One definition is a business that emphasizes adopting cloud computing platforms as the foremost means of delivering IT services and the value from them. One example of a cloud-first strategy is implementing a hybrid disaster recovery routine:

- A. Maintain a regular **local image backup** of operating systems, applications and databases on site
- B. Generate and store an **offsite backup daily** as protection against failures at facilities

This **BUDR configuration** uses cloud tech to enable rapid restoration in the wake of a cyber disaster like a ransomware breach. Also, this model underlines the largest challenge facing executives working to transform into cloud-first companies: escalating cybersecurity requirements.

How can leaders synch cloud security measures with their pace of cloud adoption?

1. **Assess readiness** by auditing devices and verifying internet connectivity/network accessibility
2. **Review policies** for acceptable use of devices, levels of privilege for access and response to breaches
3. **Establish safeguards** such as multi-factor authentication (MFA) for devices, virtual private networks (VPNs) for access and continuous monitoring for incursions

We have cybersecurity experience and expertise to walk you through this process repeatedly. Give us a call.

## Viewpoint

### MSPs Foster Organizational Resilience

Surveys by consulting firm McKinsey & Company show 84% of business leaders report feeling unprepared for future disruption. What types of disruption?

- **Economic** like rising inflation
- **Operational** like supply chain snags
- **Environmental** like natural disasters

And one type of disruption that cuts across all three categories is cybercrime, which represents risk in each case above:

- Protecting against and recovering from cyber incursions continue as **rising costs**
- Recovering from data breaches can **delay delivery** of products and strain quality of service
- Catastrophes **amplify cyber vulnerabilities** like working remotely

That's why leaders also list "resilience" among their top strategic priorities. In short, resilience is an organization's ability to anticipate, endure and recover from crises like those listed earlier. In the physical world, these catastrophes can be caused by multiple factors beyond a company's control, such as wildfires and hurricanes. In the virtual realm, the most common culprit is cybercrime.

What are the principles of cyber-resilient cybersecurity?

- **Proactive Protection** – address persistent vulnerabilities with vigilance
- **Rapid Recovery** – plan and practice your response before emergency strikes
- **Full-Speed Flexibility** – anticipate adapting in flow at high speeds

Call us for a consultation.

## IT Strategy

### Co-Managed IT Fortifies Resilience

In a recent insurance industry poll of 500 risk management professionals, nearly half of respondents identified cybercrimes like ransomware as the most prevalent source of business disruption, generating the most significant financial burdens.

These are particularly vexing findings for leaders at established small- to medium-sized businesses (SMBs) that spar with agile startups at one end of the competitive spectrum and big corporations with deep pockets at the other.

How can SMBs weather the rigors of economic volatility like fluctuating inflation, operational turmoil like supply-chain complications and environmental instability like natural disasters and maintain resiliency? We believe **co-managed IT** is the answer. It's a suite of technology services that:

- Ensures **24/7/365 service** for customers and employees
- Enhances efficiencies to advance **digital transformation (DX)**
- Expands your **infrastructure** without incurring new expenses or multiplying vendor agreements
- Enables strategy and **innovation** by filling gaps in internal technical skillsets
- Elevates and modulates **service levels** to match your escalating requirements

As a premier managed services provider (MSP), we have gained the knowledge to co-manage IT from our experiences working for an array of clients operating in diverse industries across the country. While you tackle trending challenges, we keep your tech infrastructure running smoothly in four critical areas: servers and networks, email and messaging, backup and recovery (BUDR) and cloud computing.

Visit our blog for more trending technology articles at [TeamLogicIT.com/blog](https://TeamLogicIT.com/blog).