TIP SHEET

Crafting a BUDR Strategy

When we think of IT emergencies and disaster recovery, we often think of weather-related events such as hurricanes and tornadoes. But every company, no matter your risk for natural disasters, needs to prioritize backup and disaster recovery (BUDR) plans.

From natural crises like hurricanes and pandemics to digital disasters such as system crashes and cybercrimes, potential business disruptions abound. And with most companies requiring 24/7 access to mission-critical information, your business must be ready to respond to an array of events that can interrupt your operations.

A BUDR strategy is essential. If you haven't given much thought (or action) to BUDR, begin by asking these four critical questions, which will help prepare your company's response to an IT emergency:

1. **What BUDR procedures, solutions and maintenance programs are in place?** Are backups automatic and on a regular frequency? Are you backing up all servers, workstations and mobile devices? Are you administering this process smoothly and effectively? And considering your cloud or hybrid environment?
2. **Can you trust your current BUDR procedures, solutions and maintenance routines?** When was the last time you reviewed your procedures? Have you tested your backup process or refined the maintenance regimen lately?
3. **How fast can you recover from a business disaster?** What types of threats does your business face? Are you at high risk in any category? How might bad actors disrupt your systems? And for how long might you be at risk—hours? Or days?
4. **How much will downtime cost your business?** What are the likely tangible costs of downtime for your company in terms of revenue loss or equipment repair or replacement? What are your intangible costs? Diminished productivity? Customer dissatisfaction? Damaged reputation?

It can be a sobering exercise to forecast the possible magnitude of an IT disaster, but it's necessary to consider worst-case scenarios in crafting your response strategy.

We recommend following a six-step process in the wake of a disaster:

1. ***Assess the problem:*** How many systems are affected? How much data is lost?
2. ***Establish recovery goals:*** What's an achievable day and time objective?
3. ***Select recovery path:*** Which systems come first?
4. ***Confirm functionality:*** What's working where for whom?
5. ***Complete restoration:*** There's more than one path to full recovery.
6. ***Assess afterwards:*** Review, revise and refine for next time.

Of course, the best time to consider these issues is before catastrophe strikes. Once you have given some thought to your potential risks and reviewed your current procedures (assuming you have some), give us a call for consultation. We'll walk through answers with you and help guide your BUDR planning to the next level so that you're ready for any emergency that Mother Nature, cybercrooks or sheer bad luck presents you with.

Move forward with **The Color of Confidence®.**

TeamLogicIT.com