StorageCraft

Five Top Tips

for Disaster Preparedness

Tip #1: Make a Disaster Recovery Plan

Downtime caused by a disaster, whether its hurricanes, floods, earthquakes or wildfires, results in loss of productivity and revenues. Moreover, it causes damage to an organization's brand and reputation. The average cost of downtime is estimated at around $5,600 per minute, rounding to about $300K per hour, according to Gartner.

While data protection remains crucial, organizations need to adopt a restore and recover mentality. At the most basic level, this means you must create a disaster recovery plan to ensure data is always safe, accessible, and optimized when needed and instantly recoverable in the event of an outage.

Tip #2: Don't Overlook ROBO/HO

When it comes to protecting and recovering data, organizations have always been more focused on the data center—not the edge. But due to the COVID-19 pandemic, this has changed, as a large number of employees are working remotely. The need to manage backup and recovery across remote office and branch office (ROBO) locations—as well as an increasing number of home offices (HO)—is more important than ever.

In the wake of a disaster, ROBO/HO locations put corporate data at greater risk. Security on remote networks is typically far weaker than security on corporate networks. Furthermore, remote employees have a habit of leaving their workstations unattended and their data unsecured, making organizations more vulnerable to cyberattacks. Fortunately, with the right tools and mindset, companies can easily and effectively manage their data protection in ROBO/HO locations.

Tip #3: Put Data Recovery to the Test

You need to know if your business can survive a data outage and quickly recover lost data. Regular testing of your backup system is critical to provide assurance of your ability to recover in case of data loss. The reason is simple: you don't want to find out that your backup wasn't set up correctly on the one day that you really need it.

Yet, at too many businesses, this testing never happens. Organizations and IT staff must make it a habit to periodically test their backup copies to ensure they can reliably restore data.

Tip #4: Establish your Recovery Time Objective

Downtime and lost data can cause nearly as much damage to a business as the disaster itself. A recovery time objective (RTO) is a critical tool for disaster recovery planning. It helps you understand the kind of recovery strategies and technologies you need to have in place to successfully recover from a disaster.

RTO is a measurement of your tolerance for downtime enabling you to assess how long you can go without access to your data before the impact on your organization is too great. Once you determine that metric, you're in better position to plan your recovery.

Tip #5: Embrace Cloud-based Backup and Recovery

Local backups are usually enough to recover IT systems from server failure and other common problems. But a site-wide disaster will destroy those backups and result in major downtime and data loss for a business.

When disaster strikes, ensuring business continuity is the most pressing issue for all organizations. Yet, the results of a recent survey showed that only 15% of organizations can recover from a severe data loss within an hour.

The cloud is theoretically as far away from your primary data storage as it gets making it your best and last line of defense. And it doesn't matter where your infrastructure is located if your data is backed up to the cloud. With StorageCraft Cloud Services your data is always safe, encrypted, and secure, and 99.999% available with one-click failover from anywhere.

StorageCraft