ChannelproNetwork

Disaster Recovery and Business Continuity Planning: Is the Cloud the Ultimate Answer?

Disasters lurk. But the cloud provides numerous benefits that don't exist in on-site or in-house infrastructures, and it reduces your overall level of risk. By Christopher Stark

October 18, 2012

Every business needs a solid disaster recovery plan. It is the key to ensuring business continuity through any potential disaster. Recent industry studies have found that businesses that lose their data in a disaster (hurricane, earthquake, tornado, and so on) are likely to go out of business within the next few years.

Beyond natural disasters, businesses also have to worry about technological disasters such as DNS attacks, network outages, and Internet service interruptions. In the event of a disaster of any kind, your company's and your customers' survival depends on a pre-established disaster recovery plan; network uptime; and your ability to back up, secure, and restore all vital data and applications. Do you feel confident in the services available to you and your clients?

When Control = Risk, It's Time to Let Go

Traditional disaster recovery plans were controlled by in-house staff and required redundant on-site infrastructures with mirror configurations located off-site to ensure geographic disparity. However, these solutions were not only costly, but were often only separated by a few miles, which increased the risk of a total loss in the event of a regional disaster.

With the proliferation of cloud services, an alternate front runner in disaster recovery has emerged. The cloud provides a multitude of benefits that are non-existent in on-site or in-house infrastructures, and it reduces your overall level of risk. With enterprise-class data centers powering your cloud computing solution, you will be assured near-instantaneous restoration of company-wide data and applications with only an internet connection.

This is because a quality cloud provider will ensure its system won't go down. With redundant servers, power supplies, and service providers; geographic disparity; and checks and balances to account for the "human-error factor," there's always another system at the ready to take over if the primary is taken out by a disaster.

Location, Location, Location Doesn't Matter

Location may not matter, but multiple locations do. When managing disaster recovery on-site, a major stress factor is maintaining two identical infrastructures in nearly the same location. Though your back-up site may be on the other side of town, that won't matter when a tornado, hurricane, or earthquake takes out the entire town. Not to mention the number of hours you will spend driving from one location to the other just to confirm that both systems are functioning correctly.

Wouldn't it be better if you could rely on a single point of contact with your cloud provider to guarantee continuous backup, 30-day file retention, zero downtime, enterprise-class security, and expert engineers working 24x7x365 to ensure the system is running properly—with multiple locations? Add in multiple layers of physical, logical, and methodical redundancy and suddenly you have an iron-clad disaster recovery plan that allows you to focus on more strategic IT projects.

Peace of Mind with Enterprise-class Security

To ensure data and applications are maintained appropriately, it's important to utilize U.S.-based data centers that abide by federal, state, and local security laws. The data centers should be Tier 4 certified and SAS 70 compliant with multiple redundancies, adhere to the Federal Information Processing Standards (FIPS 140) security requirements for validation, and employ the Twenty Critical Security Controls for overall security standards.

With the Cloud, you benefit from first-class virus and hacker protection and advanced technological tools to protect you from data tampering. Around-the-clock hardware and software monitoring from data-security experts ensures the prevention of issues before they occur, giving you the time and bandwidth to focus on other priorities.

Cost: Internal Disaster Recovery vs. the Cloud

Shrinking budgets are resulting in limited IT funds. With the ongoing costs of maintaining internal hardware, software licensing, and IT staff, those funds can be spread quite thin. A cloud solution offers a cost-effective, scalable alternative to internal disaster recovery with predictable

monthly expenses based on the number of users and applications, and amount of data storage necessary. In addition, the cloud provider can maintain software licensing for you as part of your agreement.

The best way to survive a disaster is to be prepared for it. Don't let the threat of a flood, virus attack, tsunami, or network outage put your company or your customers' businesses at risk of going out of business from the loss of data. Let the cost-effective, reliable, and secure cloud be the ultimate answer to your disaster recovery and business continuity needs.

CHRISTOPHER STARK *is the founder, president, and CEO of Cetrom Information Technology Inc., a provider of cloud solutions for more than a decade, with headquarters in Vienna, Va.*