

Perparing for the worst: Effective IT disaster recovery planning

Hurricane season is in full swing, but it's not too late to start preparing your business for possible storm impact or even worse, a disaster. Hurricane experts have predicted that the 2011 Atlantic hurricane season will be above average, and there is a 72 percent chance that at least one major hurricane will make landfall on the U.S. coastline.

Because data availability and security is a top priority, it is essential to develop a disaster recovery plan. Here are some helpful tips for effective disaster recovery planning:

■ **Devise a plan.** Define what is important to keep the business running – i.e., email and application access, database backup and computer equipment – and how quickly the company needs to be up and running post-disaster. Other key plan components to consider are determining who in the organization declares the disaster, how employees are informed that a disaster has occurred and the method of communicating with customers to reassure them that the company can still service their needs.

■ **Monitor implementation.** It is critical to monitor the plan to ensure its components are implemented effectively. A disaster re-



TECH 4 BIZ

Robert
Cini

covery plan should be viewed as a living, breathing document that should be updated frequently, as needed.

■ **Test disaster recovery plan.** An under-tested plan can often be more of a hindrance than having no plan at all. The ability of the disaster recovery plan to be effective in emergency situations can only be assessed if rigorous testing is carried out one or more times a year in realistic conditions by simulating circumstances that would be applicable in an actual emergency.

■ **Make password access available.** Though password protection is a key goal for data security, you need to store passwords in at least two geographically separate, secure locations. Make sure that more than one IT staff person has access to all passwords and codes. And be sure to change passwords promptly if key personnel leave the company.

■ **Perform off-site data backup and storage.** Any catastrophe that threatens to shutter a business is likely to make access to on-site data backup impossible. The primary concerns for data backup are security during and accessibility following a crisis. There is no benefit to creating a back-up file of valuable data if this information is not transferred securely and stored in an offsite data storage center with foolproof protection.

■ **Perform data restoration tests.** The backup software and the hardware on which the da-

ta resides needs to be checked daily to verify that backups are completed successfully and there are no pending hardware problems.

Companies need to store tape backups in a secure and accessible off-site location, while disk systems need to have an off-site replication if the backup is not initially run off-site. Companies should also perform monthly test restoration to validate that a restoration can be accomplished during a disaster.

■ **Back up laptops and desktops.** Although many companies have policies requiring employees to store all data on their network, users often store important files on local systems. Backing up laptops and desktops protects this data in the event of a lost, stolen or damaged workstation. Using an automatic data protection and recovery solution is ideal.

■ **Have adequate backup power.** If your facility is affected by a widespread outage, you may find yourself without power for an extended period of time. Be sure to purchase the longest-life, most uninterruptible power supply available. Then obtain additional battery backup for continued power.

■ **Be redundant.** Establishing redundant servers for all critical data and providing an alternate way to access that data are essential components of an organization's disaster recovery planning. Having these services in place at a secure, off-site location can bring disaster recovery time down to minutes.

■ **Install regular virus pattern updates.** IT infrastructure is one of those realities of business life that most companies take for granted. Companies often do not focus on email security until an incipient virus, spyware or malware wreaks havoc on employees' desktops. Organizations need to protect their data and systems by installing regular virus pattern updates as part of disaster recovery planning, which may help prevent a crisis.

If developing and managing a disaster recovery plan is too cost prohibitive or you lack adequate technical staff, consider hiring a managed services provider. MSPs have the technical personnel to design, implement and manage such projects. They have the server, storage and network infrastructure to manage a true disaster recovery plan.

The bottom line: Every business is vulnerable to a serious unforeseen disaster, and hopefully yours will never have to experience it. But, should something happen, having an effective disaster recovery plan in place will give you peace-of-mind and enable your company to recover more quickly and effectively, hopefully avoiding significant interruption and loss.

ROBERT CINI, a CPA and director in Boca Raton with CBIZ Connexia, holds the certified in technology professional (CITP) designation from the American Institute of Certified Public Accountants. E-mail him at rcini@cbizgl.com.