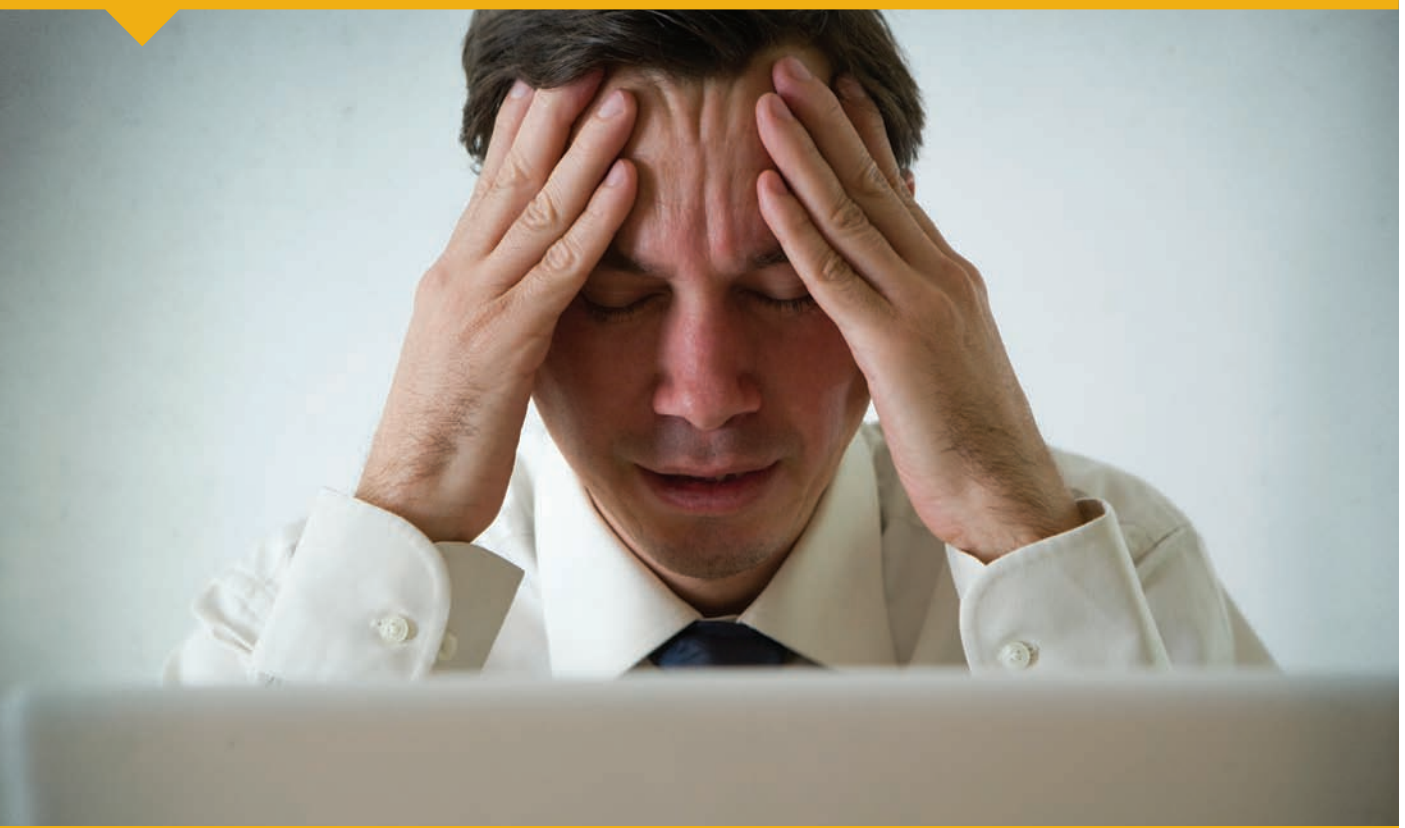

DISASTER PLAN.

NEW TECHNOLOGIES PUT FRESH WRINKLES IN BUSINESS-CONTINUITY/DISASTER-RECOVERY PLANNING.

In the IT world, disasters come in all shapes and sizes. These can include everything from Category 5 hurricanes, to power outages caused by a nearby construction site.

»»»

Nearly one-third of IT managers say they have had to implement some part of their disaster-recovery plan in the past year. This is according to a recent survey of 1000 respondents by Symantec Corporation released in August 2008.

It's no wonder that Business Continuity/Disaster Recovery (BC/DR) remains a growing concern for companies of all sizes. In fact, upgrading capabilities in this area was ranked as one of the most critical IT themes by end-user IT decision-makers at several hundred North American and European enterprises, according to Forrester Research's Data Center Infrastructure Survey.

Business continuity/disaster recovery requires a holistic approach that includes storage, infrastructure, servers, applications, middleware and the network. If that weren't complicated enough, today's new technologies are testing traditional methods of backup and data protection.

Murphy's Law exempts no one. In light of new technologies, it's time to take another look at your BC/DR plan.

» VIRTUALIZATION FACTOR

The word virtualization has become a catch-all phrase for many types of technology that make more efficient use of server space as well as storage assets. It can also bring these assets under a single management umbrella with a single point of control.

Half of the IT managers surveyed by Symantec Corp. say they are running mission-critical applications on virtual servers. However, virtualization adds a new wrinkle to the traditional model of protecting data.

Some 55 percent of IT managers surveyed by Symantec say their company is reevaluating disaster-recovery plans due to virtualization. In North America, 64 percent of companies are looking at the effects of virtualization on disaster recovery.

In some cases, virtualization is being deployed for business-continuity/disaster-recovery purposes and applications. And according to the Symantec survey, data in virtual environments poses a difficult challenge since processes for physical environments may not work in virtual environments.

"If you put 12 or 20 machines on a virtual server and attempted to run 20 backups at the same time, the pipes just aren't big enough," says Marty Ward, senior director of product marketing at Symantec. "So you have to find a unique way of doing it."

What's more, you have to keep track of where specific data is being stored. That way it can be located and restored following a disaster.

"It's almost like taking a dirty room and stuffing everything that's out of place into a closet," says Ashish Nadkarni, principal consultant at Glasshouse Technologies Inc. "You really need to put things back into their place."

» VIRTUAL MACHINE RECOVERY

Several vendors offer solutions to storing and recovering Virtual Machines (VMs). Symantec's Veritas NetBackup for VMware, for instance, can back up one to three virtual machines sitting on one physical server. For servers with four to eight VMs, NetBackup PureDisk, a data deduplication solution, can compress and reduce the amount of data before it is stored.

«« Some 55 percent of IT managers surveyed by Symantec say their company is reevaluating disaster-recovery plans due to virtualization.

In extreme cases, where as many as 80 virtual machines are housed on a single server, companies can use Symantec's VMware Consolidated Backup interface. The software allows you to take a snapshot of the entire machine.

A snapshot is a locally retained point-in-time image of data. The snapshot is indexed offline through a mapping technology, so if a single document needs to be retrieved, it can be located and recovered quickly.

Snapshot technology also wins when it comes to Recovery Point Objectives (RPO), says Bob Passmore, vice president of research and storage analyst at Gartner Inc. in Stamford, Conn.

"When you do backup to tape or virtual tape, you do it once a day," he says. "Data could end up 24-hours old. With a snapshot, you can do it once every half hour. So when you do a recovery, the data is less than an hour old." Snapshot technology also meets the most stringent Recovery Time Objectives (RTO), he adds.

An RTO is the duration of time within which a business process or data must be restored following an outage. An RPO describes the acceptable amount of data loss, measured in time, that can be tolerated following an outage.

NetApp Inc.'s snapshot technology can take hourly snapshots. EMC, HP and IBM also have snapshot capabilities, but with lower volume capacity. Some products back up less often, such as every four to six hours, Passmore says.

Despite the benefits, widespread adoption has been slow. "We don't yet have that universal piece of software, like tape backup, that works with everybody's hardware," he adds.

This is similar to Continuous Data Protection (CDP). Also called continuous backup, this is a storage system in which all the data in an enterprise is backed up whenever any change is made.

In effect, CDP creates an electronic journal of complete storage snapshots, one storage snapshot of every instant in time that data modification occurs. A CDP system with disk storage offers data recovery in a matter of seconds.

Another major advantage of CDP is that it preserves a record of every transaction that takes place in the enterprise. IBM and other vendors offer CDP products.

CDP products can be implemented as either software or hardware. Software-based CDP is more common and includes tools like Backup Exec 10d for Windows Servers from Symantec. Software is installed and configured on a host server and uses storage resources currently available in the data center.

» DATA DEDUPLICATION

The debate between backup disks vs. traditional tape has escalated. This is due to to deduplication technologies, which are making disks more affordable because companies can store more information on fewer physical disks than ever before.

As more corporate data is moved to spinning disk, storage administrators must implement, configure and manage this growing capacity — stretching disk space to the limit while protecting important data against loss or theft. Compression, deduplication and encryption are emerging in disk storage.

"I've seen an increase of deduplication requests by approximately 75 percent as compared to the same time last year," says Ravi Pendekanti, vice president of worldwide sales and marketing at Overland Storage in San Diego.

He credits budget constraints to the uptick. "We've got to do a lot with less," he says.

"How do we provide the right SLAs [Service Level Agreements] to our customers and do it in a more efficient manner by ensuring that less capacity has to be used up to provide the same level of service.

"Now you don't want 'X-Number' of copies [of backups] but just one." Another factor, IT staffs are now more educated about the technology well enough to deploy it, he adds.

File deduplication is a space-saving technology intended to eliminate duplicate files on a storage system. By saving only one instance of a file, disk space can be significantly reduced.

Deduplication can also provide more granular control. It does this by removing redundant portions of files — potentially down to the block level.

"Businesses are looking much more seriously now at reducing or downsizing their reliance on tape infrastructures as the primary backup and recovery medium," says Rob Emsley, senior director of product marketing at EMC Corp. in Hopkinton, Mass. "They are moving to more of the disk-based solution."

Deduplication can be accomplished through software or appliances. Two years ago, the two technologies battled for the best compression ratios. But today, industry-watchers contend that the two are just about equal.

"Today it's about recovery speed, recovery performance and scalability, says Symantec's Ward. The firm's PureDisk deduplication software integrates with NetBackup for storage-optimized data protection for data center, remote office and virtual environments. The deduplication engine can be deployed within NetBackup or independently using a PureDisk client.

Overland Storage offers an in-line processing approach to deduplication with its REO 9500D deduplicating Virtual Tape Technology (VTL) appliance. In October, the company also unveiled REO Compass, a disk-based appliance that combines block-based data deduplication with compression and Advanced Encryption Standard (AES) to transport data between locations with minimal bandwidth and maximum security.

EMC offers deduplication capabilities in several of its products. EMC Avamar is a combined hardware and software solution for source-based deduplication.

It is used in addition to an existing software backup application — like those in remote offices and data management environments. "You get the benefits not only of storage efficiency, but it reduces the amount of backup data that you have to copy over the network. So remote offices with bandwidth constraints and VMware environments benefit," Emsley says.

EMC's Disk Library 3D Series and DL4000 Series Disk Library, designed for target-based deduplication, plugs into an existing infrastructure, such as an IBM Tivoli storage manager. "When you save backup data to that device, it duplicates that and allows you to retain more backups in the same storage footprints," Emsley adds.

» BACKUP AND ARCHIVING CONVERGENCE

Convergence represents a bright spot amid all the changes occurring in storage and data recovery. "The world of archive and backup are very closely tied," says EMC's Emsley.

"It comes down to the ability to recover and retrieve info in an appropriate way and in an appropriate time."

Therefore, many backup products also feature archiving capabilities and vice versa. For instance, many deduplication appliances include replication — from remote offices or data centers to core storage locations. Or they can replicate data to an offsite location or a disaster-recovery site.

Overland Storage, for instance, offers Enterprise Data Replicator (EDR) as an option in its Snap Servers. "If a customer wants to do replication across the network or WAN, they have that capability with EDR," Pendekanti says. "They can not only do file system management, they can also use EDR and unlock the data duplication feature set."

Also, the company's new RealCompass data replication appliance plugs into a businesses existing IT infrastructure. "If you want to do data protection over the WAN, you can use RealCompass. It gets the data pumped on the other side of the network where it can be stored at a remote site," Pendekanti adds.

» REFINE YOUR STRATEGY

With these and other new IT developments, it's more important than ever to refine your BC/DR strategy. Take a step-by-step approach.

Each year, it's important to reevaluate which applications are deemed mission critical, business critical and less critical. This is because their importance to business operations may have changed over the years.

"I'm not sure if five years ago anyone would consider [Microsoft] Exchange mission critical, but now almost everyone does," Symantec's Ward says. For example, a commercial real estate firm has labeled Exchange as mission critical because it's used to track real estate contracts. "If that goes down, they lose deals," he adds.

Mission-critical applications are those where the business would be at a complete standstill if these systems were not in line. These applications call for data replication between two sites.

Business-critical applications are those that would disrupt business, but not shut it down. Less-critical applications, that don't require 24x7 availability, can usually be preserved with backup to tape and transporting the backup tapes to an offsite location.

Applications that require 24x7x365 availability should also have data replication, clustering or mirroring. For the most mission-critical applications, data should be replicated continuously between two sites.

Mirroring is similar to real-time replication and protects the data. However, it works in conjunction with clustering technology that helps firms failover to an alternate site when needed.

Business-critical applications should also use replication, according to Forrester Research Analyst Stephanie Balaouras. However, instead of clustering, companies can manually restart the application at an offsite facility.

Applications that are less critical to business operations can be restored through the most convenient method. These can include backup to tape or disk storage.

» OFFSITE DISASTER RECOVERY

Collocation facilities, where companies share data backup space at a highly secure facility with an uninterrupted power supply, can be invaluable if a disaster strikes. However, if data needs to be restored in hours instead of days, a more dedicated business-continuity/data-recovery strategy is required.

It will necessitate a more dedicated infrastructure, such as a remote SAN, according to Gartner Inc. Companies with immediate recovery needs should consider building their own facilities or looking at other specialized recovery site suppliers who can meet their needs. Above all, companies must continually revisit disaster-recovery plans and ask, "What if?"

"A strategy and a plan are only as good as the details put behind it," Gartner's Passmore says. "Every little hole moves the disaster forward and extends reach," he adds. "Teams have to continually ask, 'What can go wrong?' And they need to create a plan to avoid that." ◊

DISASTER RECOVERY:

The ability to make some or all stored data available following a disaster. The more difficult task of reconstructing business continuity also needs to be addressed.

BUSINESS CONTINUITY:

A plan for backing up the data directory along with the accompanying application, thereby allowing the business to get back up and running with minimal delay.