

# COMPUTERWORLD

## Backing up the edge

**Thanks to remote data replication and disk-based backup technologies, the data center is reasserting control over branch-office backups.**

**Lucas Mearian**

**August 23, 2004** -- Mike Lucas, IT director at Hogan & Hartson LLP, had had enough. The Washington-based law firm was paying \$30,000 a month to back up data on more than 400 servers located in 27 offices worldwide and store the tapes off-site. Lucas says he couldn't stomach the cost of buying more tape drives to back up every new print, file or application server.

Along with the increasing costs, the tape-based infrastructure created administration issues, including the need to sometimes rely on nontechnical staffers to swap out tape cartridges in each remote office every night and take them off-site.

Then there were the software glitches. "We'd have trouble from time to time with a tape getting hung, having to do a reboot of a server during off hours. We were at risk of not having a backup," Lucas says, adding that retrieving tapes for restoring data in an emergency could take more than a day.

Data protection executed at remote sites is often a hit-or-miss scenario because "no one knows if the backup actually happened or if a restore can occur," says Arun Taneja, an analyst at Taneja Group Inc. in Hopkinton, Mass.

Those frustrations led Lucas to use a remote backup strategy that brings backup data into the data center, where it can be centrally managed. Vendors offer a variety of network-based schemes that pull data across a WAN to a central repository. These systems are simpler to manage and more cost-effective than local tape backups, analysts say.

Most include software and appliances that replicate data from branch offices to the data center, where it is backed up to a disk device and/or tape library. This

model eliminates the need for media handling or IT support at remote sites and offers greater security, since backup data is centralized.

The increasing popularity of these systems is starting to affect sales of entry-level tape drives commonly used to back up direct-attached storage. IDC in Framingham, Mass., is forecasting a 20% decline this year as administrators increasingly decide not to back up branch servers locally.

## **The Options**

Vendors offer several approaches to remote backup. Software such as Veritas Software Corp.'s Storage Replicator and CYA Technologies Inc.'s HotBackup first execute a complete backup of direct-attached storage on each remote server or network-attached storage appliance and then move incremental or "delta" changes over the WAN to the data center.

Some organizations with branch offices that host multiple servers are choosing to first consolidate backups to a local disk-backup appliance before replicating data across the WAN. The appliance can complete server backups quickly across a LAN and then stream updates over the slower WAN connection to the data center, where it can be archived to tape.

For workstation backups, some storage administrators are creating virtual drives on remote end-user PCs and mapping those to a file server back in the data center. To avoid performance problems over the WAN, administrators install a local data-caching appliance that gives users access to their files at LAN speeds while updates stream in the background to the back-end appliance in the data center.

Lucas contracted with DS3 Data Vaulting LLC, a service provider in Fairfax, Va., for his network backup system, which includes disk-based appliances and software from Asigra Inc. in Toronto. Asigra's Televaulting DS-Client software runs on servers, desktops and laptops connected to each remote office LAN and automates the backup of about 3TB of compressed data from local backup appliances in 10 offices over the WAN to an AT&T data center. After completing an initial full backup, the remote appliance provides updates only for changed data blocks. It eliminates duplicate files, encrypts the data and compresses it at a 2-1 ratio before automatically sending it across the WAN on a scheduled basis.

Lucas expects a two-year payback on his investment. The initial system installation in Hogan & Hartson's central office cost about \$13,000. He has deployed 10 offices to date and is continuing to roll out the technology.

## **Caching Up**

Companies such as Actona Technologies Inc. (recently acquired by Cisco Systems Inc.), Riverbed Technology Inc., Disksites Inc. and Tacit Networks Inc. use appliances at both the remote site and the central data center for global file sharing. The appliances speed up access to shared files in part by removing the overhead associated with file-serving protocols such as the Common Internet File System and Network File System.

Mukesh Shah, director of network services at The Associated Merchandising Corp. (AMC) in Plainfield, N.J., is in charge of file-sharing operations among 40 remote locations in a worldwide network that includes data center hubs in Hong Kong and New Jersey.

AMC uses MetaFrame serverware from Fort Lauderdale, Fla.-based Citrix Systems Inc., which gives Windows XP PCs and wireless devices virtual, thin-client access to applications running on back-end servers. It also uses the New Jersey data center for global file sharing of Excel spreadsheets, Microsoft Word documents and other files.

But users in Asia and Europe were waiting more than two minutes for remote files to open. The system also lacked adequate file-locking safeguards for some shared files. Users were "quite unhappy," Shah says.

Eight months ago, Shah began piloting a caching appliance from South Plainfield, N.J.-based Tacit Networks in his New Jersey data center. File-access times dropped from an average of 122 seconds to 11 seconds on first access and eliminated the end-user wait altogether on subsequent attempts after the file was loaded into the local appliance's cache.

"Tacit has a process where you can push files to a local cache on a scheduled basis," Shah says. "So when users go to access the file, it's already there."

When users change and save the file back to the cache, it's also saved on the main file-sharing server in New Jersey, where AMC staffers back it up. "All restores can be done centrally, whereas if we had to substitute the cache appliance with a file server, we'd have the complexity of backups and restores at the remote office level," Shah says.

## **Outsourcing It All**

Overworked IT organizations that don't have the time or resources to set up a remote backup system can consider similar offerings from service providers.

Brian Asselin, IT director at Harborside Healthcare Corp., a Boston-based long-

term care company, oversees operations for 55 locations and 8,500 employees, but he says he has only one IT person for each of the nine states in which facilities are located.

Harborside had been using direct-attached tape backup for its remote application servers, but Asselin says ensuring that backups occurred and performing restores were a nightmare.

"Our people working in the facilities are definitely technically challenged," he says. "Logistically, it would be impossible to restore with the people I have."

What's more, the Health Insurance Portability and Accountability Act requires greater security around patient information than Harborside's IT infrastructure can provide, Asselin says. "There's just a slew of security that needs to be in place by 2005 for HIPAA," he says.

Instead of building a central data center where data could be replicated for disaster recovery purposes and further burdening his IT staff, Asselin chose service provider AmeriVault Corp. in Waltham, Mass., to host backup data storage and handle daily replication from the remote sites.

AmeriVault installed its CentralControl software on Harborside's desktops and an agent on each of its servers. After completing an initial full backup of all data, the vendor performs daily, incremental, encrypted backups over the Internet to its disaster recovery centers.

In an emergency, administrators at Harborside can perform data restores, even from home, using a point-and-click application on AmeriVault's Web portal. Alternatively, data can be shipped on tape for large restores.

Asselin says AmeriVault has "processes and procedures" that are HIPAA-compliant, which relieves his staff from having to set up its own compliance program. And Asselin says he also reduced labor costs by outsourcing his remote backup and recovery architecture because "we don't have to have people running around dedicated to the task of backup."

But while the remote backup technology made processes more efficient, the outsourcing approach wasn't necessarily cheaper.

"In terms of actual backup cost, it's pretty much a wash. When you consider bandwidth and license payments for software, it's pretty much even with other backup solutions," Asselin says.

Tony Asaro, an analyst at Enterprise Storage Group Inc. in Milford, Mass., says the costs of edge network backup technologies are continuing to drop, and as large companies investigate using these systems, big vendors are stepping in with new products.

Asaro points to EMC Corp.'s entry-level Clariion AX100 array, which can be directly attached to its NetWin 110 NAS Gateway or bought as a preconfigured storage-area network with backup and storage management software for remote office backup.

And EMC's Legato RepliStor replication software is bundled with switches from Brocade Communications Systems Inc.

"I don't think it's a fad," Asaro says. "I think more people are going to adopt this technology because it's cost-effective."