

Always Be Prepared

By Leslie Kramer

August 22, 2005

Backup data centers are an integral part of all financial institutions. An extraordinary amount of time and money goes into developing them, which includes finding the right location, using the appropriate technology, changing processes to incorporate the new facility and testing. Unfortunately, on Sept. 11, 2001, Wall Street was given a stark reminder of the importance of maintaining disaster recovery sites.

Now, more than ever, as acts of terrorism continue to be perpetrated around the world, and natural disasters, such as hurricanes, earthquakes and floods, threaten the nation's coastlines, financial institutions need to make sure that their information is secure. Most firms have gone to great lengths to safeguard their data, establishing up-to-date data recovery facilities powered by leading-edge technology and systems. But for many, the process is ongoing, as firms continue to figure out the best way to set up secure and reliable backup data centers.

Few institutions know more about the importance of having a safe and functioning backup site than Boston-based Putnam Investments. Its sister company, insurance brokerage firm Marsh, which is owned by parent Marsh & McLellan Companies, lost close to 300 people the day the Twin Towers fell, and many of those lost were technologists. "Quite frankly, we had a baptism by fire a few years ago," says Philippe Bibi, chief technology officer at Putnam. "The data center was completely vaporized, if you will, so we had to respond for our sister company, Marsh," he adds.

Since the companies are run independently, Bibi relates, Putnam technicians did not have any prior knowledge of Marsh's systems. As a result, it took Putnam about four business days to recover Marsh's critical systems.

To ensure business continuity, Mellon Financial Corp. maintains two primary, redundant data centers located in Pittsburgh. Currently, however, Mellon is doing due diligence on a new data recovery site, which it plans to build in Western Pennsylvania. The firm hopes to have the facility up and functioning by 2007.

Location, Location, Location

Mellon's primary reason for choosing the location of the new site was that it wanted to increase the physical separation between its two computer facilities in Pittsburgh, while at the same time maintaining its capabilities with respect to synchronous data replication and recovery of all its applications, according to Frank Dittrich, senior vice president of information technology services at Mellon. Dittrich notes that while some firms may elect to use an asynchronous state of replication, which allows for increased geographic dispersion, "The down side is that it puts your

primary data center and your recovery site out of sync in terms of the data - by minutes to hours - depending on how the companies elect to configure themselves," he says.

In choosing and designing the new site, Mellon considered the ability of its network to connect the two data centers via high-speed connections, as well as the capacity of the new facility's storage system and its ability to protect the data. The center also has to support high-volume transactional systems, Dittrich notes.

Additionally, Mellon looked at the probability of natural disasters in the region and the quality of the infrastructure. "We had to be aware of where railroad lines ran, where hazardous material is carried, where the airports and nuclear power plants are, and how the site would be affected by natural events that can impact Western Pennsylvania, such as heavy rains and winter storms," Dittrich explains.

In choosing the location of its data recovery site, New York-based John A. Levin & Co. weighed the location of its employees. The firm chose to establish its newest data recovery site in Connecticut, where it has been up and running since April 2003. The facility is more than 50 miles away from the firm's main location, but it is close enough to where many of the firm's employees live so that they could reach the facility should they need at some point to work out of the site, notes Mark Sanders, chief technology officer at John A. Levin & Co.

The fully operational facility performs full data replication of all of John Levin & Co.'s business systems on a daily basis, Sanders relates. It does not perform real-time replication on all of its databases, but instead performs data dumps or data copies once a day. "If anything happens during the normal work day, the worst case scenario would be that we would lose whatever work was done during that day," Sanders says. "The best case would be we would potentially lose only what happened in the last hour."

The firm does, however, use real-time data replication for its most sensitive data, such as trading information, Sanders stresses. "That changed the whole production environment, because most of our core business systems are in a multinode cluster, and it doesn't require replication at that point," he explains. "But to get the tertiary device to be part of the same environment, but physically in a different place, we had to use Veritas replication software." (Veritas recently merged with Cupertino, Calif.-based Symantec Corp.)

The creation of the new data recovery site presented Levin & Co. with an opportunity to upgrade its original servers to support the additional computing capacity for real-time replication, Sanders notes. The firm was able to use the older equipment at the disaster recovery site. Now, users have improved performance, while at the same time mitigated risk, Sanders asserts. "It is the most cost-effective disaster recovery site I have ever built, and I've built a few," he says.

Mirror, Mirror

Putnam, now well versed in disaster recovery, has opted to take a three-pronged approach to its data protection. The firm has developed two primary data facilities located 70 miles apart in cities outside of its headquarters in Boston. "As our first level of defense, within each data center we have clusters and very sophisticated platforms that allow us to deal with a server going down or a disk failing or even loss of commercial power," says the firm's Bibi. Both data centers are live and connected through sophisticated, highly available fiber networks that are self-healing, he

explains. "So if one data center goes down, the other center, in a seamless fashion, will be able to support all of our business needs and systems, through data center mirroring," Bibi continues.

Putnam uses Hopkinton, Mass.-based EMC's DMX technology to mirror the data for its critical applications between the two sites, giving it a second layer of protection. As a third level of protection, Putnam backs up all its information on tape at the end of each day and sends them off-site to a service provider to be stored in an underground bunker. It also contracts with SunGard to provide recovery services out of region.

Of course, the enormous investments in backup facilities and systems are valuable only if the systems actually work. To ensure that they do, most firms test and monitor constantly throughout the year. "We are testing all the time to be sure that our recovery capabilities are working properly; this is important because we've learned that when we had backup machines that were used only in the event of a problem, quite often they were not actually ready to work, and that costs you time," says Mellon's Dittrich.

Even if all systems are go, most institutions still constantly examine emerging technologies and new ways to store and recover data in the event of a disaster. "It's based on continuous process improvement," says David Ficke, managing director of enterprise computing at Putnam. "We develop our plan, we test our plan, we learn from the test and then we add that information into the new plan." The hope, however, is that the firm never again will have to execute it.