Users assess plans for data protection, disaster recovery

Network World, Oct 31, 2005 by Connor, Deni

ORLANDO - Amid the devastation of Hurricane Wilma last week, IT professionals appraised their disaster-recovery and data-protection plans and said their strategies are in flux, regular testing is necessary and funding is still hard to get.

At the Storage Networking World conference last week - attended by more than 2,000 IT professionals - a panel of users said that although disaster recovery and data protection head their lists of IT priorities, funding is often elusive, and many of their strategies are in transition as their storage and application infrastructure changes.

Funding a disaster-recovery scheme is difficult, said Hal Weiss, systems engineer for Baptist Memorial Health Care in Memphis.

"One of the major issues of a hospital organization is that we are constrained by the amount of money we get because we depend on Medicare and Medicaid to reimburse us," he said.

Weiss said his disaster-recovery plan is limited, because he is not involved in determining which applications the organization purchases.

"I can't pick the applications the organization uses, because they are controlled by the clinicians," Weiss said. "Sometimes an application doesn't lend itself to a disaster-recovery strategy?

Weiss has a 138T-byte storage-area network (SAN) and is experiencing a 300% annual increase in data that needs to be protected. For backing up the data on his SAN and disaster recovery, he uses Revivio's CPS 1200 continuous data protection array and Copan's Revolution 200T array.

Money for disaster recovery is often denied because businesses don't understand its necessity.

"Recovery has always been kind of a 'Johnny One Note' business process," said John Toigo, moderator of the panel and senior analyst for Toigo Partners in Dunedin, Fla. Management "sees it as spending money on a set of procedures that don't yield any tangible benefits to the company," he said.

John Gideon, business continuity manager for Rent-a-Center in Piano, Texas, has received funding for disaster recovery and has created an out-of-state hot site for his business-critical and financial applications.

"Our finance systems are replicated in real time [between locations] and will come up in different stages depending on the application," Gideon said.

At Auto Warehousing inTacoma,Wash., CIO Dale Frantz also has set in motion a plan to test his disaster preparedness.

"We have 28 facilities and we test at a specific facility once a month," Frantz said."Our tests involve pulling out drives in the server to watch the failover process and make sure it works."

Al Todd, senior vice president of IT for Pacific Capital Bancorp in Santa Barbara, Calif.,also tests his disaster recovery plan regularly While Todd uses a service to protect his data, he plans to bring his disaster recovery onsite in the next year.

"We take data [annually] from our offsite storage facility and have it flown out to the site, download the data onto a machine at the site, attach it to the SAN and prove we can run our systems remotely from Philadelphia," Todd said. "We are now in a transition to several times a year testing and will bring our disaster recovery in-house."

Todd has a SAN consisting of two Hitachi Data Systems TagmaStore Universal Storage arrays, each with 20T bytes of storage, two Hitachi 9585V arrays with 20T bytes of storage, as well as IBM and EMC storage arrays. The SAN connects to as many as 200 Intel-based servers, each with 200G bytes of direct-attached storage, and a mainframe.