

Disaster recovery planning: How do you measure up?

By **Liz Gold**

(April 16, 2007) - When Matt Camden, chief information officer at UHY Advisors in Chicago, faced an audit server outage in one of his New England offices over a February weekend, he was able to restore his data in a period of 11 hours.

"Two of our disks failed, which is a terrible thing to happen," Camden recalled. "All we had to do is put new server hardware in place, which is our responsibility, then we got the data back up, loaded it, and it worked like a charm." He credited his online data protection company, EVault, for the rapid restoration process.

Unfortunately, too few companies are well-prepared for an emergency - and the results can often spell the end of a business.

In a January study conducted by the Economist Intelligence Unit, the U.S. National Archives and Records Administration reported that 25 percent of companies that experienced an IT outage lasting from two to six days went bankrupt immediately. That same report also revealed that 93 percent of companies that lost their data center for 10 or more days filed for bankruptcy within a year.

"Years ago, it used to be talked about if you experienced a disaster, but in today's environment, we talk about when you experience one," said Ben Thornton, director of disaster recovery and business continuity planning for Norcross, Ga.-based Optimus Solutions, a provider of IT infrastructure support products and services. "You've got to make that worst-case assumption that you will have to deal with a disaster or significant business interruption."

Disaster recovery planning, a component of business continuity management, isn't a new concept, but experts say that more companies are opening their eyes to the importance of a holistic plan that keeps a business resilient.

Whether it's the threat of natural disasters, such as hurricanes or earthquakes, or man-made ones such as employee sabotage or terrorism, it's critical that companies not only have a plan, but implement it.

"When people talk about business continuity, it's less about the technology and more about the kind of plan they put in place, the processes, and how they make sure the businesses can continue to work and operate," said Dan Lamorena, senior manager of product marketing for a data center management unit of Symantec, a global information security concern in Cupertino, Calif. "Disaster recovery tends to talk about what you would actually do in terms of technology. As more companies move to IT and move away from being manual, it's really important they understand what those technologies are to help them recover as quickly as possible."

THE CHANGING FACE OF DISASTER

Natural disasters, technology failures or deliberate acts by outsiders all can be devastating to a company.

"To a user, they can think of losing a critical file as a personal disaster," said Ellen Rome, vice president of sales and marketing at StorServer, a Colorado Springs, Colo.-based company that focuses on online data protection back-up, archiving and disaster recovery. "Customers are now looking at recovery point objectives, meaning, 'If I can get back to what my data looked like yesterday, then I'm

fine,' and recovery time objectives, meaning, 'If I can get it up and running in a day if I have a disaster, then I'm good.' We help determine what their need is."

Thornton said that he defines a disaster from the standpoint of the effects of that particular disaster, not from the perspective of what caused the disaster. "The disaster occurs when you have an inability to perform your critical business functions within an acceptable period of time," he said. "To me, that's very expressive, because it really introduces two issues: One, what is critical, and two, what is an acceptable period of time. And that varies by every company."

Still, Thornton said that he has seen a shift take place over the last 15 years to less "predictable" disasters. He defined predictable disasters as hurricanes, fires and other natural disasters. "You start injecting the malicious intent of terrorists, [and] it's a whole different threat level that is challenging us," Thornton said. "If you looked at a pie chart portraying the various disasters that occurred 10 to 12 years ago, you wouldn't see terrorism on there. You might see a little bitty blip or it might be included under 'other.' Today, it's got its own slice of the pie."

According to Joyce Bastoli, senior vice president at Ajilon Finance Solutions, a finance, accounting and operations consulting company in Saddle Brook, N.J., the financial loss that resulted from the 9/11 attacks was "a big wake-up call for many companies."

"The biggest driving force in creating a business continuity plan is loss of revenue," Bastoli said in an e-mail. "A plan must be able to continue the flow of funding, as well as keeping clients and customers served as they would be under normal circumstances. Loss and damage to a business is serious, and the threat of disaster, be it natural or otherwise, should be taken as such."

DUST OFF THAT PLAN

Many experts agree that awareness of the importance of business continuity among companies has increased over the past few years, but according to Karl Kispert, solutions director for technology risk management at Jefferson Wells in Parsippany, N.J., the interest to follow through hasn't necessarily been steady.

"We were in the bottom of the valley," Kispert said, of interest in disaster recovery planning prior to the terrorist attacks on the World Trade Center. "September 11 came [and] we were in the peak. Everybody wanted to do it. Time heals all wounds. Three years ago it was back in the valley, but then along came Sarbanes-Oxley. Even though Sarbanes-Oxley doesn't mandate you have to pay attention to disaster recovery and business continuity management, part of what the CEOs and boards were saying was that, 'If we have a disaster, we can recover because we are responsible for the financial stability of the company.'"

But awareness does not mean that companies are prepared to fend off potential threats, or that they have a viable plan in place to protect their people, technology and information.

According to Kispert, Jefferson Wells measures a company's disaster-planning capability on a maturity model where zero means chaos and five means optimal. He has found that most Fortune 500 companies rank at one. "They have some stuff," he added, "But they don't have enough to really resume business."

Jim Bourke, CPA, CITP and partner-in-charge of internal technology at the CPA and business advisory firm WithumSmith+Brown in Red Bank, N.J., said that he has had similar experiences in his work. "By far the biggest problem that we see is that a company's disaster recovery plan is far from current," he said via e-mail. "All too often, a company hires an expert to create the plan and then it basically sits on a shelf. We continually try to get the message across that disaster recovery plans should be living documents and should be continually revisited on a recurring basis."

Jim Grogan, vice president of product development for SunGard Availability Services, in Wayne, Pa.,

said that he has experienced a communication gap between companies' disaster recovery plans and the growth that is actually taking place within the company. He said that his company's mission is to keep an organization's staff connected to the automation they need to do their job.

"Most companies have sort of a plan in place; the difficulty that we see more often than not is that that plan has not matured to align with their business goals," Grogan explained. "The staff that is responsible for IT generally will have some sort of strategy. We find very often the thresholds that the data center is planning for don't line up with the business units. There is still a significant disconnect between the plans engineered at the data center versus the expectations of the business unit."

Whether a company already has a plan in place or is about to create one, Jefferson Wells offers seven steps as guidance when coordinating a business continuity management project.

The first step in the process is to identify and assess an organization's needs. Next is performing a risk assessment to determine a company's threats and vulnerabilities, according to Kispert.

"The company has to understand what risks they are facing," he said, adding that the third step is recognizing the impact on a company if an interruption does occur. "The risks in southern Florida are different than the risks in Montana or Illinois."

Once an impact analysis is completed, Kispert said that his company then moves on to creating a recovery strategy. A written document is prepared to use as a playbook, and finally the process moves onto its last two steps: testing and then educating and implementing other employees in the organization.

"It's best practice on a yearly basis to review your entire business continuity plan," Kispert suggested. "Twice a year you should really chunk it out and have each department review it to make sure of things as simple as the calling tree are up to date."

While resilience can be built by the small details, such as updating that calling tree on a regular basis, it's also about asking tough questions internally to make sure that companies, especially those in the financial industry, are being proactive about their protective measures.

"Can you imagine closing your books and you just realized that someone was able to maliciously go into your systems and manipulate your data? That, to me, is a big concern," Kispert said. "Maybe you're outsourcing your general ledger and all of a sudden that outsource provider goes down. How are you going to resume business? Where's your back-up capability to close your books? Sometimes you have to scare them into [thinking], 'Oh my God, that can really happen.'"

Got Technology?

Recent trends, according to WithumSmith+Brown IT partner-in-charge Jim Bourke, are revealing that more companies are backing up their data off-site with mirror-image technology in real time.

"In today's rapidly changing environment, the days of being able to go back to a set of tapes from yesterday, last week or even last month are long gone," Bourke said. "Today, if a company does not have the ability to back up real-time data, they could suffer substantial monetary losses in the event of a disaster."

Simple tactics work, too, according to Symantec senior manager Dan Lamorena. A CPA himself, he suggested off-the-shelf back-up software, investing in an external hard drive or extra disk storage, and saving that information to a different location, such as an office or a vault.

"I think what companies probably need to start looking at is management tools for their data center that have the ability to use a portal interface and tools that allow you to migrate workloads across various geographies," Lamorena said. "More and more companies are going to have to have these types of tools that before people thought were a little expensive. Now they are going to find these are a necessity."

More choices in technology have brought some of the cost of these tools down, according to SunGard vice president Jim Grogan.

"A few years ago, everything was tape-based," he said. "Today, companies have a much wider choice of technology that would allow them to have fail-over systems where the data is already geographically remote, copied or replicated in real-time. Having that technology available gives a broader array of choices and the market has brought the prices down."

Richard Heitmann, EVault's vice president of product marketing, said that lower product costs have increased adoption of his company's services. "The cost of disk drives continues to plummet, so that obviously makes a disk-based back-up solution much more appealing," Heitmann said. "We've seen the availability of bandwidth continue to grow both in terms of amount and how much data you can send over the Internet. Companies, in general, [are] much more educated. What we're seeing is much greater awareness and much greater understanding of the technology and the benefits technology can bring."