Sponsored by Zenith Infotech Ltd

# BACKUP AND DISASTER RECOVERY

As the digital universe grows beyond imagination, enterprise IT executives face the daunting task of keeping their little pieces of it backed up and recoverable. They must keep on their toes – this exercise isn't to be done once and forgotten. As the company evolves, adding different types of data to its stockpiles and becoming increasingly virtual, so too must its backup and disaster recovery strategy. In these articles, *Network World* and its sister publications *CIO, Computerworld, CSO* and *InfoWorld* lay down the groundwork and explore the latest tips and technologies for no-fail corporate data backup and disaster recovery.

## IN THIS eBOOK

# ABC: AN INTRODUCTION TO BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

**CSO and CIO staff, CSO, March 6, 2007**

## Understanding the basics will go a long way in preparing for everything from minor nuisances to major catastrophes

Disaster recovery and business continuity planning are processes that help organizations prepare for disruptive events – whether an event might be a hurricane or simply a power outage caused by a backhoe in the parking lot. Management's involvement in this process can range from overseeing the plan, to providing input and support, to putting the plan into action during an emergency. This primer explains the basic concepts of business continuity planning.

**Q: “Disaster recovery” seems pretty self-explanatory. Is there any difference between that and “business continuity planning?”**

**A:** Disaster recovery is the process by which you resume business after a disruptive event. The event might be something huge, like an earthquake or the terrorist attacks on the World Trade Center, or something small, like malfunctioning software caused by a computer virus.

Given the human tendency to look on the bright side, many business executives are prone to ignoring “disaster recovery” because disaster seems an unlikely event. “Business continuity planning” suggests a more comprehensive approach to making sure you can keep making money. Often, the two terms are married under the acronym BC/DR. At any rate, DR and/or BC determines how a company will keep functioning after a disruptive event until its normal facilities are restored.

**Q: What do these plans include?**

**A:** All BC/DR plans need to encompass how employees will communicate, where they will go and how they will keep doing their jobs. The details can vary greatly, depending on the size and scope of a company and the way it does business. For some businesses, issues such as supply chain logistics are most crucial and are the focus on the plan. For others, information technology may play a more pivotal role, and the BC/DR plan may have more of a focus on systems recovery. For example, the plan at one global manufacturing company would restore critical mainframes with vital data at a backup site within four to six days of a disruptive event, obtain a mobile PBX unit with 3,000 telephones within two days, recover the company's 1,000-plus LANs in order of business need, and set up a temporary call center for 100 agents at a nearby training facility.

But the critical point is that neither element can be ignored, and physical, IT and human resources plans cannot be developed in isolation from each other. At its heart, BC/DR is about constant communication. Business leaders and IT leaders should work together to determine what kind of plan is necessary and which systems and business units are most crucial to the company. Together, they should decide which people are responsible for declaring a disruptive event and mitigating its effects. Most importantly, the plan should establish a process for locating and communicating with employees after such an event. In a catastrophic event (Hurricane Katrina being one example), the plan also will need to take into account that many of those employees will have more pressing concerns than getting back to work.

**Q: Where do I start?**

**A:** A good first step is a business impact analysis (BIA). This will identify the business's most crucial systems and processes and the effect an outage would have on the business. The greater the potential impact, the more money a company should spend to restore a system or process quickly. For instance, a stock trading company may decide to pay for completely redundant IT systems that would allow it to immediately start processing trades at another location. On the other hand, a manufacturing company may decide that it can wait 24 hours to resume shipping. A BIA will help companies set a restoration sequence to determine which parts of the business should be restored first.

Here are 10 absolute basics your plan should cover:

1. Develop and practice a contingency plan that includes a succession plan for your CEO.
2. Train backup employees to perform emergency tasks. The employees you count on to lead in an emergency will not always be available.
3. Determine offsite crisis meeting places for top executives.
4. Make sure that all employees, as well as executives, are involved in the exercises so that they get practice in responding to an emergency.
5. Make exercises realistic enough to tap into employees' emotions so that you can see how they'll react when the situation gets stressful.
6. Practice crisis communication with employees, customers and the outside world.
7. Invest in an alternate means of communication in case the phone networks go down.
8. Form partnerships with local emergency response groups – firefighters, police and EMTs – to establish a good working relationship. Let them become familiar with your company and site.
9. Evaluate your company's performance during each test, and work toward constant improvement. Continuity exercises should reveal weaknesses.
10. Test your continuity plan regularly to reveal and accommodate changes. Technology, personnel and facilities are in a constant state of flux at any company.

**Q: Hold it. Actual live-action tests would, themselves, be the "disruptive events." If I get enough people involved in writing and examining our plans,**

**won't that be sufficient?**

**A:** Here's an example of a company that thinks tabletops and paper simulations aren't enough. And why its experience suggests it's right.

When Steve Yates joined USAA, a financial services company, as CIO (he has since left the company) business continuity exercises existed only on paper. Every year or so, top-level staffers would gather in a conference room to role-play; they would spend a day examining different scenarios, talking them out – discussing how they thought the procedures should be defined and how they thought people would respond to them.

Live exercises were confined to the company's technology assets. USAA would conduct periodic data recovery tests of different business units, like taking a piece of the life insurance department and recovering it from backup data.

Yates wondered if such passive exercises reflected reality. He also wondered if USAA's employees would really know how to follow such a plan in a real emergency. When Sept. 11 came along, Yates realized that the company had to do more. "Sept. 11 forced us to raise the bar on ourselves," says Yates.

Yates engaged outside consultants who suggested that the company build a second data center in the area as a backup. After weighing the costs and benefits of such a project, USAA initially concluded that it would be more efficient to rent space on the East Coast. But after the attack on the World Trade Center and Pentagon, when air traffic came to a halt, Yates knew it was foolhardy to have a data center so far away. Ironically, USAA was set to sign the lease contract the week of Sept. 11.

Instead, USAA built a center in Texas, only 200 miles away from its offices – close enough to drive to, but far enough away to pull power from a different grid and water from a different source. The company also made plans to deploy critical employees to other office locations around the country.

Yates made site visits to companies such as FedEx, First Union, Merrill Lynch and Wachovia to hear about their approaches to contingency planning. USAA also consulted with PR firm Fleishman-Hillard about how USAA, in a crisis situation, could communicate most effectively with its customers and employees.

Finally, Yates put together a series of large-scale business continuity exercises designed to test the performance of individual business units and the company at large in the event of wide-scale business disruption. When the company simulated a loss of the primary data center for its federal savings bank unit, Yates found that it was able to recover the systems, applications and all 19 of the third-party vendor connections. USAA also ran similar exercises with other business units.

For the main event, however, Yates wanted to test more than the company's technology procedures; he wanted to incorporate the most unpredictable element in any contingency planning exercise: the people.

USAA ultimately found that employees who walked through the simulation were in a position to observe flaws in the plans and offer suggestions. Furthermore, those who practice for emergency situations are less likely to panic and more likely to remember the plan.

**Q: Can you give me some examples of things companies have discovered through testing?**

**A:** Some companies have discovered that while they back up their servers or data centers, they've overlooked backup plans for laptops. Many businesses fail to realize the importance of data stored locally on laptops. Because of their mobile nature, laptops can easily be lost or damaged. It doesn't take a catastrophic event to disrupt business if employees are carting critical or irreplaceable data around on laptops.

One company reports that it is looking into buying meals ready-to-eat (MRE) from the company that sells them to the military. MREs have a long shelf life, and they don't take up much space. If employees are stuck at your facility for a long time, this could prove a worthwhile investment.

Mike Hager, former head of information security and disaster recovery for OppenhiemerFunds, says 9/11 brought issues like these to light. Many companies, he said, were able to recover data, but had no plans for alternative work places. The World Trade Center had provided more than 20 million square feet of office space, and after Sept. 11 there was only 10 million square feet of office space available in Manhattan. The issue of where employees go immediately after a disaster and where they will be housed during recovery should be addressed before something happens, not after.

USAA discovered that while it had designated a nearby relocation area, the setup process for computers and phones took nearly two hours. During that time, employees were left standing outside in the hot Texas sun. Seeing the plan in action raised several questions that hadn't been fully addressed before: Was there a safer place to put those employees in the interim? How should USAA determine if or when employees could be allowed back in the building? How would thousands of people access their vehicles if their car keys were still sitting on their desks? And was there an alternate transportation plan if the company needed to send employees home?

**Q: What are the top mistakes that companies make in disaster recovery?**

**A:** Experts note the following pitfalls:

1. **Inadequate planning:** Have you identified all critical systems, and do you have detailed plans to recover them to the current day? (Everybody thinks they know what they have on their networks, but most people don't really know how many servers they have, or how they're configured, or what applications reside on them — what services were running, what version of software or operating systems they were using. Asset management tools claim to do the trick here, but they often fail to capture important details about software revisions and so on.

2. **Failure to bring the business into the planning and testing of your recovery efforts.**

3. **Failure to gain support from senior-level managers.** The largest problems here are:
   – Not demonstrating the level of effort required for full recovery.
   – Not conducting a business impact analysis and addressing all gaps in your recovery model.
   – Not building adequate recovery plans that outline your recovery time objective, critical systems and applications, vital documents needed by the business, and business functions by building plans for operational activities to be continued after a disaster.
   – Not having proper funding that will allow for a minimum of semiannual testing.

**Q: I still have a binder with our Y2K contingency plan. Will that work?**

**A:** Absolutely not (unless your computers, employees and business priorities are exactly the same as they were in 1999). Plus, most Y2K plans cover only computer system-based failure. Potential physical calamities like blackouts, natural disasters or terrorist events bring additional issues to the table.

**Q: Can we outsource our contingency measures?**

**A:** Disaster recovery services – offsite data storage, mobile phone units, remote workstations and the like – are often outsourced, simply because it makes more sense than purchasing extra equipment or space that may never be used. In the days after the Sept. 11 attacks, disaster recovery vendors restored systems and provided temporary office space, complete with telephones and Internet access for dozens of displaced companies.

**Q: What advice would you give to IT executives who need to convince their CEO or board of the need for disaster recovery plans and capabilities? What arguments are most effective with an executive audience?**

**A:** Hager advises chief security officers to address the need for disaster recovery through analysis and documentation of the potential financial losses. Work with your legal and financial departments to document the total losses per day that your company would face if you were not capable of quick recovery. By thoroughly reviewing your business continuance and disaster recovery plans, you can identify the gaps that may lead to a successful recovery. Remember: Disaster recovery and business continuance are nothing more than risk avoidance. Senior managers understand more clearly when you can demonstrate how much risk they are taking.

Hager also says that smaller companies have more (and cheaper) options for disaster recovery than bigger ones. For example, the data can be taken home at night. That's certainly a low-cost way to do offsite backup.

**Q: Some of this sounds like overkill for my company. Isn't it a bit much?**

**A:** The elaborate machinations that USAA goes through in developing and testing its contingency plans might strike the average IT executive (or CEO, anyway) as being over the top. And for some businesses, that's absolutely true. After all, HazMat training and an evacuation plan for 20,000 employees is not a necessity for every company.

Continuity planning comes down to basic risk management: How much risk can your company tolerate, and how much is it willing to spend to mitigate various risks?

In planning for the unexpected, companies have to weigh the risk vs. the cost of creating such a contingency plan. That's a trade-off that Pete Hugdahl, USAA's assistant vice president of security, frequently confronts. "It gets really difficult when the cost factor comes into play," he says. "Are we going to spend $100,000 to fence in the property? How do we know if it's worth it?"

And-make no mistake-there is no absolute answer. Whether you spend the money or accept the risk is an executive decision, and it should be an informed decision. Half-hearted disaster recovery planning is a failure to perform due diligence. •

Contributing writers include Scott Berinato, Kathleen Carr, Daintry Duffy, Michael Goldberg, and Sarah Scalet.

# CASE STUDY: HURRICANE KATRINA DISASTER RECOVERY LESSONS STILL POPPING UP

**Paul Desmond, Network World • May 6, 2008**

## Tiering applications, paying attention to people issues are key

For at least three days prior to when Hurricane Katrina struck, Marshall Lancaster and his IT team at Lagasse were closely tracking the storm, hoping it would spare his company's New Orleans-based headquarters and data center but preparing for the worst. By the time Katrina made landfall early on a Monday morning in August 2005, Lancaster and his team were in Chicago at the company's backup data center, having already declared a disaster.

Marc Benioff, the CEO of SaaS CRM vendor Salesforce.com, recently explained just why his flavor of the cloud computing model was best suited for today's troubled eco nomic times. Forget big contracts with Microsoft, Oracle or SAP, and get beyond outdated hardware and software solutions, Benioff told CNBC in early October. Benioff said that Salesforce.com's "pay-as-you-go, elastic model" offers clients much more flexibility.

At the time, Lancaster was an IT executive with Lagasse, a subsidiary of United Stationers, where he now serves as vice president of IT, Enterprise Infrastructure Services. While Katrina ravaged New Orleans, Lagasse experienced no system down time. In fact, the day after Katrina hit, the company recorded its second-largest sales day, and its third-largest the day after that.

Lancaster related his Katrina experiences at a Network World IT Roadmap event in Chicago, which the New Orleans native now calls home. He spoke of the need to consider the people element in disaster planning and how when a disaster strikes, it bears little resemblance to any pre-planned disaster recovery drill.

"When an event occurs, it isn't just about whether or not your systems come back online, but where's everybody going to be?" Lancaster said.

### Anatomy of a disaster

Lagasse was battle-tested by the time Katrina rolled in, having experienced four hurricanes in the previous few years: Isadore and Lilli in 2002, Ivan in 2004 and Dennis earlier in 2005. Indeed, the company had the drill down pat.

On Thursday, Aug. 25, Lancaster and his team began to take serious note of Katrina by implementing a "Level 1 inclement weather policy," Lancaster said. That basically just tells employees the company is tracking the storm.

# BAPTISM OF FIRE

**"There's no better test than actually doing it and running your business that way," Lancaster said of the [Hurricane] Ivan experience. "This wasn't testing. This was real live fire."**

The next day, the company went to Level 2, which is when it tells its associates to make sure their homes are in order, with sufficient supplies of food, water and the like. "We were still pretty hopeful [Katrina] was going to veer," he said.

By Saturday morning, Aug. 27, the five computer models Lagasse was tracking all showed the storm pointed at New Orleans. The only question was whether it would be a direct hit. But Katrina was by now so powerful that even a glancing blow was likely to mean substantial damage.

The company declared a Level 3 emergency that morning, which meant planning for the headquarters and data center to be closed on Monday morning. Critical personnel had to be transported to somewhere safe, with access to communications.

Those critical personnel included Lancaster and his IT team, who headed to Chicago to make sure the company's backup systems were ready. "We still had a lot of unfounded optimism that this storm would pass us by and we would be spared," he said.

By that night, with all meteorological models showing Katrina making a direct hit on New Orleans, that optimism was gone. "At 8:55 p.m., we decided to declare a disaster." That means turning on the disaster recovery platforms and using them going forward. By midnight, all Tier 1 applications were online and tested. By 7:33 p.m. the next day, all Tier 2 applications were available. "That means all customer-facing business capacity was online and working."

At 6:10 a.m. on Monday, Aug. 29, Katrina made landfall in New Orleans. From Chicago, Lancaster and his team monitored their New Orleans data center, to see whether the backup generators and other redundant features in place would keep it operational. "Less than an hour and a half after the storm arrived, our New Orleans data center went dark," Lancaster said.

## Advanced preparation

What enabled Lagasse to survive Katrina was a practical plan forged by the trial and error from the previous hurricanes. "I can learn if I'm hit over the head by things and that's what happened in this case," Lancaster said. When Hurricanes Isadore and Lilli hit in 2002, the company's disaster plan included assumptions that didn't pan out. Things were better by the time Ivan hit in 2004, when the company was forced to declare a disaster and run its operations from the Chicago backup site for five days.

"There's no better test than actually doing it and running your business that way," Lancaster said of the Ivan experience. "This wasn't testing. This was real live fire."

One of the lessons learned was the importance of coming up with the tiering strategy that dictates the order in which applications are brought back online following a disaster. Lancaster sought to come up with tiers that are easy to understand and communicate to the business side.

Tier 1 applications are those specifically required to generate revenue. For Lagasse, that means the ability to take, pick and ship orders. The goal is that such applications suffer no more than 15 minutes of data loss and be recovered within six hours. "That was deemed acceptable by the business, especially considering we're maintaining a low cost profile," he said, noting the organization's IT budget was just 0.8% of revenue.

These applications also should be recoverable through semi-automated means and without assuming that specific, highly knowledgeable people are available. The use of scripts and detailed documentation meant personnel with good IT knowledge would be able to recover the resources, but it didn't necessarily require the same people who work with them every day, he noted. Applications such as the company ERP system were consistently replicated to the Chicago site via a 3Mbps frame relay link.

Tier 2 applications are those that have to do with the customer experience. Essentially, that means anything that customers would notice if it were down, such as online order entry and various reporting applications. For these applications, the company is willing to lose as much as 24 hours of data and live with a recovery objective of three days. Less automation is involved in recovering these resources and it can be difficult without specific IT staffers.

At Tier 3 are computing resources used only internally, that won't be noticed by anyone outside the company. "They'd only hurt us," Lancaster noted. The IT group makes no specific commitment as to when it will recover Tier 3 applications, he said.

"Spending a lot of money and adding a lot of complexity to become very good at recovering Tier 3 applications really wasn't very value added," Lancaster said. "We'd rather hit the Tier 1 and Tier 2 [applications] 100% and worry about the Tier 3 when the time comes."

Post-Katrina, Lancaster said some adjustments were in order in terms of how applications were classified. Financial systems, for example, fit the Tier 3 definition. But Katrina hit in late August, and September is the last month of the quarter. By Sept. 8, Lancaster was hearing from the CFO about Securities Exchange Commission regulations.

Likewise, e-mail was originally classified as a Tier 3 application. But in the wake of Katrina, "We found e-mail to be about the most valuable communication tool we had at our disposal," Lancaster said. "It very quickly escalated to Tier 1."

Another key to Lagasse's successful disaster recovery plan was keeping its application architecture simple. Whenever possible, his group strives to be involved in defining the solution to a business need, rather than having solutions forced on it. "When an application gets forced on you, it often has architectural principles that are not aligned with what you do, and so you're not very good at [supporting the application]. It just makes things a lot harder," he said.

A few specific technologies were also crucial to the Lagasse recovery effort: VoIP, VPNs and thin clients. VoIP enabled Lagasse to create call centers virtually anywhere, including in its shipping facilities and warehouses, by simply dropping phones in. Call agents could go to these facilities and appear to be in the same call queue as teams in the company's traditional call centers, he said.

Likewise, with VPNs and a Citrix-based thin client capability, displaced staffers who had access to an Internet connection could become productive again. "Every user who had a laptop became a productivity worker the instant they could find a wire," Lancaster said.

### The people part

One of the more difficult aspects of coming up with a disaster recovery plan is accounting for individual employees after disaster strikes. "The people element is largely missing in every conversation I've ever had about this subject," Lancaster said.

When companies perform disaster recovery tests, it normally involves booking flight reservations and hotel rooms months in advance. As the event draws closer, staffers argue about where to get drinks the night following the event. At the event itself, everyone gathers around a big table and lets each other know when their bit is complete, so the next step can begin.

## Disaster Recovery Tips and Lessons Learned

**Advice from Marshall Lancaster, vice president of IT, Enterprise Infrastructure Services for United Stationers, on how to implement effective – and cost-effective – disaster recovery plans.**

**Have a backup communications plan in place.** Following Hurricane Katrina, cell phones were essentially useless because they were all homed out of a New Orleans central office that was out of commission. "You could call out, but you couldn't call in. So we were able to call people, but not each other," Lancaster said. Lagasse ended up relying on its internal associate Web site to instruct employees to call an existing toll-free employee hotline in order to get in touch with them.

**Be wary of tape recovery.** "If you're going to use [tape] for anything you really care about, just make sure you understand it very well because it's complex and you need to understand what occurs if there is a problem," Lagasse said. It's best to rely on a premier storage provider for Tier 1 and 2 applications; use tape only for Tier 3.

**Be aware of force majeure clauses.** Many vendor contracts have such clauses that essentially say in the event of certain major disasters, they are not required to provide assistance – so don't count on them.

**Take advantage of technology refresh cycles.** As a way to keep costs down, move older equipment into your backup environment as you replace it.

**Use "owned space."** Lagasse's backup data center was housed in its parent company's data center, another cost-saving technique vs. leasing backup space.

**Don't try to protect against everything.** Lagasse performed scenario pre-planning to determine which events were most likely to occur at its New Orleans headquarters and what the impact would be. Hurricanes were obviously high on the list and, thus, the company focused its resources in protecting against them.

**Consolidate applications and databases.** Running multiple applications and databases on a single server is another way to reduce costs in your disaster recovery environment. "Performance requirements aren't nearly as high as you expect when a disaster recovery occurs," Lancaster noted.

*—Paul Desmond*

"That's not how it really happens," Lancaster said, noting he learned from the experience of those earlier hurricanes. "In 2002, when we asked associates to take part in disaster recovery, they said the first thing that they should say: 'I've got a husband and two kids or a wife and a kid and two dogs and I've got to do things, I've got to take care of things.' The company just fell off the priority list."

By 2004, Lagasse had strategies in place to ensure that it wouldn't ask employees to go anywhere until their families were taken care of, either by moving them to a safe location or letting them accompany employees. This was a powerful step that eliminates a lot of scrambling when a disaster occurs, enabling faster decision-making, he said. After Katrina, Lagasse employees scattered from New Orleans to areas where Lagasse had a presence – including Chicago, Atlanta and Philadelphia – and to areas it didn't, such as Tennessee, Texas and other parts of Louisiana and Florida. In some of those areas, Lagasse had sites where employees could gather while in others they worked out of homes, hotel rooms or Internet cafes.

In the end, it was those employees who made the disaster plan work. "All plans fail in the face of the enemy. We ended up with associates having to make decisions on the fly, and having to make risky, very difficult decisions on the fly," Lancaster said. "And the caliber of those people greatly determined how effective those decisions were. So hiring and development is very important." •

---

Desmond is president of PDEdit, an IT publishing company in Southborough, Mass.

# HOW TO IMPROVE DISASTER RECOVERY

**Bill Snyder, CIO • May 15, 2008**

## Tips and technologies for reducing recovery times, lowering costs and raising continuity confidence levels

Hancock Bank, a century-old institution headquartered on Mississippi's hurricane-prone Gulf Coast, likes to boast that it will be the last to close and the first to open when stormy weather shuts down area businesses. That claim got the severest test imaginable when Hurricane Katrina roared ashore in 2005. "We were hurt badly," says Ron Milliet, the bank's director of IT services.

Hancock's IT department, which serves 150 sites across four states, took a major hit, of course, but it could have been worse. The bank found that the relatively small number of servers it had virtualized (the project had just begun when Katrina hit) could be recovered in hours, while the physical servers took days, Milliet says. Many critical services were up within 24 hours.

Virtualization steals the spotlight, but it's just one of the innovative tools now available to CIOs who are rethinking their disaster recovery and business continuity strategies. Techniques including WAN optimization and appliance-based e-mail backup are reducing recovery times, lowering costs and most importantly, raising confidence levels that business will continue even after a major disaster. As for good old tape, it's still a backup mainstay, but CIOs are looking for supplementary technologies that can be used to overcome the venerable media's limitations.

Not only are CIOs adopting new disaster recovery technologies, "they are asking themselves what disaster recovery will do to improve business as a whole," says Michael Croy, director of business continuity solutions for the Forsythe Solutions Group. That could mean, for example, leveraging IT assets acquired during a merger by putting the excess capacity to work as a backup or mirror site, or making underutilized resources part of a disaster recovery arsenal.

And because there are a wealth of new disaster recovery strategies available, customers are now in a stronger-than-ever position to cut affordable and flexible deals with vendors running offsite recovery services such as SunGard and IBM, Croy says.

### The virtual solution

Gamblers look at a casino and see slot machines, roulette wheels, bars and restaurants. But for an IT exec, the same casino is a river of data and applications that must keep flowing 24 hours a day, no excuses accepted.

The Borgata Hotel Casino and Spa in Atlantic City, N.J., had been using a traditional tape backup solution, but it was "slow and inconsistent. We were in a labor-intensive manual world," says John Forelli, the resort's vice president of IT.

What's more, the tape system gobbled a significant amount of network resources, and since the 2,000-room hotel is a 24/7 business, it was difficult to find a time to back up a server without sacrificing overall performance, Forelli says.

In 2006, three years after the resort opened, management decided to virtualize its Windows servers using VMware and speed backup and recovery tasks with replication software from Double-Take Software.

Double-Take replicates application data from 77 virtual production machines to a single physical disaster recovery target and will failover to the target (automatically switch over to the backup system) in the event of an outage. When the reserve system is activated, the appropriate application services are started within a corresponding virtual machine at the disaster recovery site and users are automatically redirected, Forelli says.

Because the software looks at data on the byte level and replicates incrementally, there's less bandwidth pressure on the network. "It's automatic, it's quick, it's under the covers," he says.

That simplicity is one reason why virtualization is becoming so popular for disaster recovery. "Windows systems are miserable to recover," says Donna Scott, an analyst with Gartner.

At Hancock, Katrina's lesson that virtualization equals faster recovery, along with a corporate desire to cut hardware and power costs, convinced the company to move much of its operations to a virtualized environment (with the exception of a mainframe-based banking system). The bank replaced 55 physical servers with five blade servers running VMware infrastructure, saving $150,000 in server hardware capital costs alone, Milliet says. There, is however, a potential downside. "We have a lot of eggs in one basket. One bad motherboard can take out a lot of virtual machines at one time," he says. To avoid that disaster, Hancock uses software that automatically will switch the virtual machine workload to another physical server if trouble is detected.

## Smart WAN tricks

For companies struggling to ship large amounts of data across the network, WAN optimization can improve day-to-day performance and speed backup and recovery operations as well.

Cubist Pharmaceuticals was using a traditional disaster recovery model that involved backups to tape, a day or more of travel time to the recovery site, at times a wait for available machines and then a cumbersome restore. "Boring, static, not flexible," comments Michael Geldart, senior manager of computer operations at the company's headquarters, in Lexington, Mass.

Geldart was not only concerned about his disaster recovery strategy, he also was struggling with the large amount of data the company needed to move between headquarters and its facility in Italy.

Moreover, management wanted to use the same WAN link for videoconferencing and VoIP. Increasing the bandwidth, Geldart says, "would have been a very expensive proposition."

Cubist already had introduced virtualization, "so one of the benefits that we wanted to get was the ability to do a snapshot of these [virtualized] machines and replicate them to other sites," he says.

The company decided to move forward with a Riverbed Steelhead WAN optimization and application acceleration implementation. The major applications it needed to speed up over the link to Italy were Exchange 2003, Microsoft networking/CIFS, and for the disaster recovery link, FTP and NFS, Geldart says. With its own equipment in place at a third-party vendor's recovery site (out of state), backup and recovery time have been reduced dramatically. That's because the data is now replicated and sits on a live disk array, eliminating the need to restore from tape, which is one of the most time consuming parts of disaster recovery, Geldart says.

Tape is still useful, he adds, noting that it provides the ability to retrieve historical data and also can be a backup should replication fail.

Interestingly, deploying its own equipment at an offsite disaster recovery facility run by a third-party involved some struggle with that vendor. "The initial reaction [from the vendor] was a blank stare," Geldart says. But [the vendor] came around, and Geldart reports that "they are absolutely changing their model." (For security reasons, Cubist prefers to not reveal the name of the recovery site's vendor.)

Croy, the Forsythe consultant, agrees. Vendors in this arena, such as SunGard, are becoming more flexible and competitive, he says. However, he argues those companies still need to lower costs, become even more flexible and broaden the scope of offerings "to better meet business needs."

## E-mail appliances deliver

Backing up e-mail in case of disaster has been a costly and time-consuming problem for years, says Gartner's Scott. But now appliances are making it much easier to replicate Exchange and other major mail servers, she says.

Ken Adams, CIO of the Baltimore-based law firm of Miles & Stockbridge, says his company tried clustering Exchange servers, but found the strategy too complicated to engineer, requiring personnel to manage as well as hefty outlays for hardware and licensing. "We're a law firm, not a technology company," he says.

But the company's 600 or so e-mail accounts are considered mission-critical, so a solution was mandatory. Adams eventually turned to Teneros, which sells continuity appliances designed to replicate Exchange servers. The Teneros appliances are IP-based and easy to install at production and disaster- recovery sites, says Adams.

Should one of the firm's Exchange, BlackBerry or Goodlink servers go down, the appliance takes over. And since Teneros monitors and maintains its appliances, there's little overhead for Adams' IT group.

## Budgeting wisely

While disaster planning needs to be high on your to-do list, that doesn't mean you've got to bust your budget. In Katrina's wake, Hancock "opened the checkbooks for DR," Milliet says. "But now, we want to rationalize our spending to be in line with business value."

One way to do that is to integrate disaster recovery needs with day-to-day operations, as Cubist did by optimizing its WAN.

On a larger scale, Hancock's management realized that having a single, centralized call center in hurricane country was courting disaster, so it opened a second. Score one for disaster recovery, and chalk up a win for customer service: The new facility reduces caller wait times for customers during normal operations. •

Snyder is a freelance writer based in California.

# IS AN ONLINE BACKUP SERVICE OK FOR YOUR DATA STOCKPILES?

**Deni Connor, Network World • May 19, 2008**

## Online data backups and e-mail archiving finally turning the storage-as-a-service dream into a business reality

These days in IT, you can buy a service for anything — including, once again, your storage.

Today's storage-as-a-service providers have arisen from the ashes of the dot-com era's storage service providers (SSP). But they differ in one critical way: They want to store your backups and e-mail archives, not your mission-critical, front-line data. The new storage-as-a-service idea has gained cachet quickly among IT professionals who don't want the burden of data backups, e-mail management and content archiving.

Such holds true for Corey Grone, IT manager at the University of Pittsburgh's Graduate School of Public Health (GSPH). The backup burden has eased considerably since he began using EMC's Mozy storage-as-a-service offering, Grone says. The Mozy online backup service has helped him provide consistent backup for seven departments of varying technological sophistication.

"Our departments run the gamut, from having lots of personnel and technology infrastructure to having none," Grone says. "Using Mozy was a way for us to deploy a backup solution across the board in a straightforward, rapid and easy way without having to worry about infrastructure and personnel to man the infrastructure and all of the issues associated with traditional backup strategies," he says.

With Mozy, which EMC acquired along with Berkeley Data Systems in September 2007, Grone backs up user files on desktops and laptops nearly continuously. If users lose data, they can recover it over Mozy servers.

At first, the thought of relying on storage-as-a-service for data backups was a big concern, Grone says. His worries disappeared once he conducted his due diligence, however. Mozy won him over with such features as encryption of data in transit and at rest. In addition, Grone likes that Mozy lets users create their own encryption keys to guarantee privacy.

Online data-backup services can help out the bottom line, too. With online backup, IT departments can avoid having to invest in backup software, hardware and media, and still provide reliable data protection. Online backup services are priced in two ways — by the amount of backed-up data in gigabytes or by the number of servers, desktops and laptops backed up. For example, Mozy costs $24 for a single server license and 10GB of storage or from $30 to $70 for five servers and 20GB of storage.

At the University of Pittsburgh, the cost to the GSPH of planning, implementing and maintaining a backup infrastructure would have been prohibitive, Grone says. "Implementing Mozy sidesteps all of these concerns and presents a secure off-site backup solution that is easy to deploy and maintain," he says. "The pay-as-you-go pricing model also ensures that our costs match our utilization, providing immediate return on investment."

## Storage service evolution

Acceptance of the storage-as-a-service concept has been a long time coming. In the dot-com era, a variety of SSPs launched with the goal of providing online storage facilities for companies that couldn't develop their own storage infrastructure readily. Most SSPs, including Storability, Storage Networks and StorageWay, failed amid user skepticism about an outsider's ability to store business-critical data reliably.

A few SSPs managed to survive the bust, however, and have made the transition into the storage-as-a-service world. Two examples are online backup and archiving providers AmeriVault, now called Venyu following a merger with hosting company NTG, and Arsenal Digital Solutions. Arsenal Digital services now form the heart of IBM's storage-as-a-service offerings; IBM acquired the company in December 2007.

Besides former SSPs, storage-as-a-service providers include other longtime storage vendors and small players, too. For example, data-protection mainstay Iron Mountain became one of the first established storage companies to offer storage-as-a-service. It entered the market four years ago via acquisition, first grabbing Connected, then LiveVault. Connected provided online backup for laptops and PCs within enterprises; LiveVault aimed its services at backing up servers in the same environment.

Smaller storage-as-a-service companies, including Asigra and Robobak, offer their online backup technologies through a reseller channel of managed-service providers (MSP) and telecom companies. Asigra, for example, has expanded its Televaulting services through such MSPs as Data Store 365. Robobak, which has been offering services for remote offices and branch offices since June 2007, is building a channel through US Data Vault and Digital Fortress. IBM, though certainly not a small company, also works the managed-services channel for storage-as-a-service offerings picked up through Arsenal Digital. It offers ViaRemote for servers and PCs through its Business Continuity and Resiliency Services division and AT&T.

Last year, storage-as-a-service really started heating up. Besides EMC's acquisition of Mozy and IBM's of Arsenal Digital, HP and Symantec launched storage services of their own.

Other storage-as-a-service activity includes Autonomy's acquisition of Zantaz in July 2007 and Dell's acquisition of MessageOne, a start-up offering Microsoft Exchange server failover and e-mail archiving services. In addition, CommVault, known for its data-protection software, entered the storage-as-a-service market early this year. It offers a managed data-protection service through DBS International, Incentra Solutions and Rackspace US, as well as a remote management service.

## Storage-as-a-service buy-in

Almost half of storage-as-a-service users are in the small-to-midsize-business market, with organization such as the University of Pittsburgh's GSPH not wanting to extend their IT resources with a backup infrastructure. Larger enterprises are adopting storage-as-a-service, too, to protect data on laptop and desktop computers, IDC reports.

Storage-as-a-service appeals particularly to enterprises that need to replace or supplement faulty tape infrastructures with more reliable backup and protection technologies.

Such a need is what drew Joe Gillis, MIS manager for The Beal Companies, a real-estate management firm in Boston, to online data backup services. In the past, he would run a traditional grandfather-father-son backup rotation with daily, weekly and monthly tapes. Once a month, he'd ship the tapes off-site. "Depending on when a disaster occurred, my data could be as much as a month out of date," he says. "With the off-site archiving, you don't face that problem."

An early storage-as-a-service user, Gillis added in the AmeriVault-AV online service for remote data backups and e-mail archiving almost five years ago. "Not having to take tape home or ship it to an archiving site data protection is the primary advantage of using a storage service," he says.

For extra protection, Gillis runs backups locally, too. "To be honest, though, the restoration process from the vault is so quick and simple, there is really no advantage to having a local copy, except if the Internet happens to be down," he says.

American Warehouses also complemented tape with online data backup service. The logistics-services provider in Houston learned its lesson the hard way. After a hardware failure on one of its HP servers, the company was down for two weeks recovering the data.

"The tape drive had failed for the previous four days and had not sent us a notification to say that it was not getting a good backup," says Tony Carter, CEO of American Warehouses. "One of the applications on our server ... hosts a warehouse-management system that is the spinal cord of our operations."

Following the failure, Carter turned to online data-backup services from Terian Solutions, a reseller of Asigra's Televaulting software, to protect mission-critical applications. Downtime of any sort can't be tolerated any longer.

"If we are down for two weeks anymore, we are out of business," Carter says. That would be a pretty sad ending for a 50-year-old company. •

Connor is principal at Storage Strategies Now. She can be reached at dconnor@ssg-now.com.

## Data, data and (lots) more data

**With the digital universe growing at an unprecedented and faster-than-expected rate, storage-as-a-service options could come in handy for enterprises**

**161B GB** - amount of digital information created or replicated in 2006

**281B GB** - amount of data created or replicated in 2007

**264B GB** - amount of available storage on hard drives, tapes, CDs, DVDs and memory in 2007

**2T GB** - size of the "digital universe" by 2011

**10** - number of times greater the digital universe will be in 2011 than it was in 2006

**85** - percentage of the digital universe to which enterprises must apply security, privacy, reliability and compliance measures

# VIRTUALIZATION CALLS FOR REVISED BACKUP STRATEGIES

John Brandon, Computerworld • Feb. 21, 2008

## Which of three popular approaches is right for you?

Virtualization is causing customers to rethink their backup strategies, with technology that combines pieces of traditional and well-understood enterprise backup with some pieces that are unique in the virtualized world.

In the past, traditional enterprise backup in the vast majority of shops has included spinning disk for short-term and intermediate data use, archival tape for long-term storage, and software such as IBM Tivoli and HP StorageWorks.

But some say that's no longer enough in a virtualized world.

"You definitely can't take a wait-and-see approach with backup, especially now that more and more companies are using server virtualization in critical production environments," says Stephanie Balaouras, a senior analyst for virtualization strategies at Forrester Research. "Backup is going to become a major challenge if companies haven't explored their options."

Traditional backup systems have a one-to-one relationship with servers. These tried-and-true backup systems and associated software already support storage-area networks (SAN), fiber optics, and the latest operating system and server hardware updates. But they are not geared specifically for the complex world of virtualization, which involves multiple guest operating systems on the same box.

Dave Russell, Gartner's vice president of research for servers and storage, outlined three popular strategies for virtualization backups. The most common is putting software agents on each virtual machine (VM) and then using traditional enterprise backup software. A second approach is to create an image of the VM and either use a storage service hosted elsewhere or take daily snapshots of the logical unit number (LUN).

A third strategy is to use VMware consolidated backup (VCB) that incrementally archives the VM – meaning it copies only what has changed since the last backup. In this way, companies can restore a single file, even from one of 30 guest operating systems that all reside on a single physical server.

"Most companies gravitate toward the backup agents and traditional backup software, which they are used to doing with a physical server, and it feels very natural and easy," Russell says. "But this approach has proven to be cost prohibitive because of the number and scale of VMs and the licensing required."

Backup agents are included with VMware and other virtualization products to help administrators integrate VMs into the traditional backup process. The main advantage is cost:

## A WORLD OF POSSIBILITIES

**"The traditional method of putting a tape in a backup system serving multiple servers is outdated," says Michael Williams, ITN's executive director of IT. "Once you move to virtual storage and separation of the volume from the physical disk, you can do very interesting things."**

The agents are free or add a relatively minimal fee. On the downside, agents force administrators to use a fairly simplistic approach: Admins can archive an entire virtualized server, but not pick and choose volumes or guest operating systems. Nor can server administrators restore specific portions of data, or substantiate (verify the data integrity) of VM volumes.

### VM snapshots

A new trend is for companies to create mirrors of the VM volumes, says Russell, because it provides more flexibility, reduces costs and allows a company to substantiate an entire location, which fits into an enterprisewide backup strategy for disaster recovery.

For example, at the Immune Tolerance Network (ITN) – part of the University of California clinical research group in San Francisco – virtualization backups have become not just a part of disaster planning, but they actually help researchers with clinical trials to fight new diseases.

ITN archives the LUN, or the specific address of the hard disk drive. Using data de-duplication algorithms that weed out redundant data, it keeps multi-terabyte archives of virtual servers. Researchers can request additional archival LUNs, a process that would be difficult or impossible with physical servers.

"The traditional method of putting a tape in a backup system serving multiple servers is outdated," says Michael Williams, ITN's executive director of IT. "Once you move to virtual storage and separation of the volume from the physical disk, you can do very interesting things. The first thing we do when we provision a LUN is we oversubscribe it. A researcher believes they have 2TB volumes – and they do."

But in reality, the LUNs are thin-provisioned, or allocated just enough storage space on a physical disk, based on snapshot policies, and they might only be 20GB each. That volume of data is backed up every four hours. This is equivalent to a hard crash backup (a complete archive of data that can be restored to a prior state), Williams says.

Williams explains that the archives – created using Network Appliance's SnapShot and SnapMirror – are then moved to an off-site location in Herndon, Va., and archived further using Veritas NetBackup over a wide-area network to create a full-image backup on low-cost Serial Advanced Technology Attachment drives.

He describes the snapshot process as beneficial to the researchers because it is easier to request a restore and faster than it was in previrtualization days, but it is still complex for IT. A scientist could request a data retrieval, which is similar to a traditional storage-restore request, and not have to wait for IT to access a library of tapes and make the restore. But the virtual restore process is more complex for IT, because staffers might have to, say, find and mount a virtual LUN from a restore point located on a separate backup system, such as a Veritas archive. The end user can access the data in a matter of hours instead of the much longer time frames required by tape.

Another advantage involves data de-duplication, a process in which the backup software is smart enough to see the same data multiple times and keep only one archive of it. At ITN, for example, there are 150 virtual servers, and there may be as many as 100 Windows machines. NetApp can make one copy of an identical 8.5GB image for Windows and create a fingerprint file (a reference point) for each additional archive, which saves on disk space because NetApp does not make multiple backups of the same Windows data.

## Continuous data protection

The third popular backup strategy for virtualization is to use a continuous data protection system such as Vizioncore vRanger or PHD Technologies's esXpress.

Health First, a group of hospitals and trauma centers based in eastern Florida, is using this strategy. The company runs 300 guest machines on 19 VMware ESX servers connected to a 150TB SAN. Health First uses IBM Tivoli for traditional backup, but because of its large virtual server infrastructure, the company decided to add a continuous backup system.

"We needed faster rebuild time in case of a disaster," says Jeff Allison, a Health First network engineer in charge of virtualization planning. "We use Vizioncore vRanger for hot backups of every virtual machine we have every night," he says. "Backups start at 5 p.m. on two different machines and by 2 a.m., we have backups for 230 boxes." The remaining 70 VMs are archived by the morning, and performance for the clinical applications is "not affected by the hot backups," Allison says.

Allison explains that the environment is more demanding in terms of uptime requirements for trauma centers and clinics, because data loss at a health facility could mean loss of life.

He describes one scenario where a controller failed on one test/development physical server that caused 80 VM development servers to be unavailable and unusable until a lengthy restore process could be initiated. On average, it could take several hours, he says. With a continuous backup system, the restore would now take about an hour and require perhaps one technician instead of several.

Indiana University, in Bloomington, Ind., presents another case for continuous backups, as opposed to VM mirroring or agents, because of the faster disaster recovery time and more granular data-archiving benefits.

A VM is contained within a file that can be quiesced (archived incrementally) via a snapshot file, says Robert Reynolds, a senior software analyst at the university. "For the majority of our VMs, that quiesced file is stable enough to be then copied as a [disaster recovery] backup," he says. "Obviously, database servers and other transaction in-flight servers need more care in creating a disaster recovery backup.

"We run weekly jobs on each of our VMware ESX servers, using PHD's esXpress virtual backup appliances, to create the disaster recovery backups for our VMs," Reynolds says. "We create a copy on the local storage of the ESX server and we are in the process of developing a second phase to FTP the disaster recovery backup to another server where it will be picked up by Tivoli Storage Manager and sent offsite to Indianapolis, roughly 50 miles from Bloomington."

## A blend of approaches

"In the near term, a blend of these technologies might be the best approach – taking an image-level backup and indexing those files continuously so that companies could do a single file restore, taking snapshots very rapidly, using a traditional backup application and VM agents to index the content on servers," says Gartner's Russell. "It does add more management complexity and another layer of abstraction to traditional backup, but the storage-resource tools are now catching up." •

# CASE STUDY: HOW ONE COMPANY USED VIRTUALIZATION TO LOWER THE COST OF DISASTER RECOVERY

**Vincent Biddlecombe, CIO • June 26, 2008**

## Transplace CTO Vincent Biddlecombe shares his backup strategy

Designing a disaster recovery plan has traditionally forced companies to strike a delicate balance. To create a plan that restores operations quickly, an enterprise needs to invest significant capital. On the other hand, costs can be cut dramatically if an enterprise is willing to withstand longer periods of operations downtime. During the planning stages and while the computer network runs properly, the forces to reduce costs are felt the strongest and often prevail. But when disaster strikes and the network goes down, everyone starts screaming to get the network up and running again, as fast as possible. Finding a way to walk this tightrope is a major challenge, but with the advent of virtualization, deploying disaster recovery plans that restore operations quickly – and at a reasonable cost – is quite possible.

At Transplace, we developed a new disaster recovery plan based on virtualization when we moved our infrastructure to a new production data center in 2007. We also took that time to refresh our hardware and review our overall architecture. Previously, we ran daily backups and physically moved the data to an off-site location. With this process, we risked being down for a half day if we experienced a problem in the middle of the day. This type of plan also limited us in that we only backed-up once a day, which meant we risked losing a day's worth of work. This plan also required us to have dedicated servers that sat idle except when we executed a recovery.

After we moved into our new data center in Dallas at the end of 2007, we began to plan our new disaster recovery data center in Arkansas, into which we moved in February 2008. At the storage level, we deployed network-attached storage and SnapMirror software from Network Appliance to create virtual storage for our database and application servers. SnapMirror allows us to send copies of all changes to our backup facility on a near real-time basis without impacting the performance of the applications. Anytime a record changes in production, it sends a copy to our disaster recovery facility. This shared-storage approach also allows us to manage storage centrally. We buy storage only when we need it.

LESS IS MORE

**Enterprises should take a good look at compression technologies. With all of the data that needs to be copied to the disaster recovery site all day long, it's important to reduce the amount of bandwidth you require so that your network runs efficiently.**

At the database level, we deployed IBM P570s with AIX as the operating system, leveraging its logical partitioning technology. This combination allows us to partition each server to look like multiple servers, and we can run multiple database servers by sharing the capacity of the individual servers. In the disaster recovery facility, the database server runs four to six copies of Oracle that we use for testing and development most of the time, but if the need arises, we can shut down the virtual servers and run the disaster recovery instance of Oracle on that same server. This also allows us to make the most efficient use of our Oracle licensing costs, which are charged by each physical CPU core.

At the application server level, where we run VMware and Windows on Dell servers, the content of each virtual machine is also replicated to the disaster recovery site anytime an update occurs. With VMware and IBM database servers, we use a set of servers for testing and development. When we need to run a disaster recovery restore, we turn off the virtual servers for test and development, bring-up the ones for disaster recovery, and we're good to go. All the data and content of the servers is quickly copied over.

## Four-step disaster recovery process

For enterprises ready to develop a disaster recovery plan, we recommend a four-step process that helps frame the project and ensures a reliable disaster recovery process:

### Step 1: Enablement

Make sure all the data is properly transferring to the disaster recovery data center. Ensure that all the proper hardware in the disaster recovery data center is in place, will remain stable and is running on up-to-date operating systems. Also, review all applications and decide how long you can you go without each one. This helps prioritize the most crucial applications. Some applications might need to be restored in less than an hour while you might be able to do without others for up to 12 hours. This part of the plan becomes an internal SLA.

### Step 2: Testing

Develop detailed procedures and processes on how and how often to test the disaster recovery plan. We recommend at least once per quarter. You also need to determine how to measure success so that you can evaluate the testing and document the findings to compare one test to another with a high level of validity.

### Step 3: Cutover documentation

You need to document exactly how you will cut over if and when a disaster strikes. There will be some elements similar to the test process, but there will also be differences for how you execute procedures while under a live disaster recovery. With all the pressure your IT staff will be under, it's critical that this step be clearly and thoroughly documented.

### Step 4: Returning to normal production infrastructure

Just as important as how to cut over to your disaster recovery infrastructure is knowing how to return to your normal production infrastructure. It's not always a case of doing things in reverse, and it's a process you should also test.

### Lessons learned

It's important to bring all of the key vendors and your internal IT team into the same room at the same time. This gives everyone a chance to voice concerns, explain how their piece of the puzzle contributes to the overall project, and to understand the functions of the other parts of the project. If you get yourself into a position where you act as the go-between among your vendors, important information will undoubtedly be lost in translation.

Enterprises should take a good look at compression technologies. With all of the data that needs to be copied to the disaster recovery site all day long, it's important to reduce the amount of bandwidth you require so that your network runs efficiently.

Looking back on the disaster recovery plan we started in 2007, we feel we have achieved the ultimate balance: a simple way to recover operations fast — but at a relatively lower cost than traditional disaster recovery systems. Without a doubt, virtualization played a vital role in helping us achieve this mission. •

Biddlecombe is the CTO of Transplace. He has more than 15 years of experience in IT consulting with an emphasis on transportation management systems.

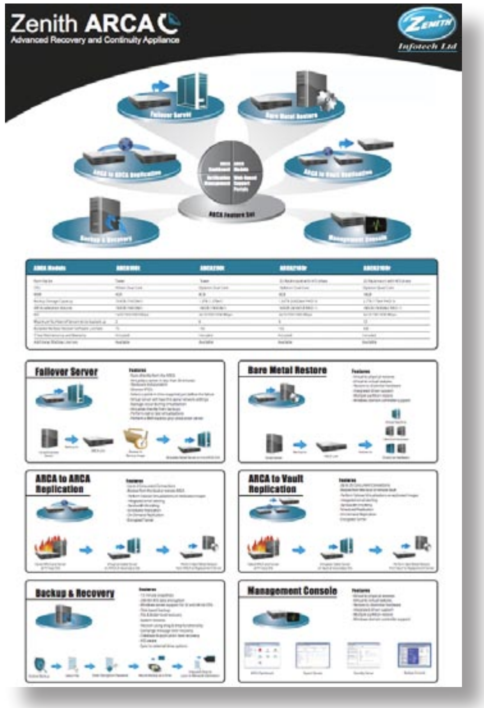
# DISASTER RECOVERY RESOURCES

## Zenith ARCA Brochure

Learn more about the feature rich business continuity appliance from Zenith Infotech

## Exchange Recovery Made Easy

Watch this demonstration on how easy it is to perform an Exchange restore with Zenith ARCA.



## Zenith ARCA Technology Poster

Download the Zenith ARCA Technology poster