CIO DECISIONS

ALIGNING IT AND BUSINESS IN THE MIDMARKET ENTERPRISE

ezine

BEYOND BACKUP

D.R. STRATEGIES FOR BRANCH OFFICES

How the latest technologies are changing disaster recovery for remote and branch offices across the midmarket.

INSIDE:

July/August 2009
Volume 7

TechTarget
The Technology Media ROI Experts

EDITOR'S LETTER

Recovery and the Remote Office

→ **I HAVE ALWAYS** been intrigued by the challenge of remote office management, probably because remote and branch offices are such a staple of midmarket companies and their growth strategies. I remember giving an award to a CIO who developed an "office in a box"—a bundle of processes and technologies that systematized setting up IT for new offices because his health care firm was opening so many. We've talked to others about batch uploads of sales data from retail outlets, outsourcing branch office IT support or the effort behind rationalizing and consolidating IT across multiple sites after a merger or an acquisition. The challenge is clear.

And so is the need to add those sites to an organization's disaster recovery plan.

Recently we wrote online about a Midwest utility that was almost up a creek (so to speak) when flooding forced staff at a regional office to quickly secure office space through some partners.

The company's disaster recovery plan focused on the headquarters office in the next state—big help that was. Yet too often, smaller offices are left without a paddle when the water rises: No advance plan about where employees should go, no certainty that backup procedures were followed and most of the data is safe.

There's no excuse for not filling that void. There are too many ways to address the problem:

- Cancer Treatment Centers of America, with four hospitals around the country, has built in five layers of redundancy.
- Advertising agency Arnold Worldwide installed SANs at its two main offices with a fat pipe between them for backup.
- Neighborhood Centers Inc. has turned to managed backup.

As our CIO mentor, the Real Niel, says inside: "Sort, document and test. That is what I do to improve the chances my remote sites will recover from what can go wrong." If he can do it, if those CIOs mentioned above can do it, so can you. ■

ANNE MCCRORY
Editorial Director
amccrory@techtarget.com

Q+A

Creating a Branch Office Disaster Recovery Plan

How the latest technologies and basic processes work together to give you cost-effective protection from outages, wherever your remote offices are. **BY KRISTEN CARETTA**

→ **WHETHER YOUR REMOTE** or branch offices are regional offices, retail outlets or far-flung outposts, there are many options for creating disaster recovery and business continuity plans that address the challenges of smaller offices and, often, light on-site IT support. We spoke with **STEPHANIE BALAOURAS**, a principal analyst at Forrester Research Inc., about the best processes, technologies and even IT computing models in use today for cost-effective disaster recovery for data and applications at remote sites. Balaouras also gives advice on how much you should be spending.

How does a company create a disaster recovery plan for its remote and branch offices?
[You] need to have local DR plans that address the risks for the region. The remote office is going to have to document the plans, test the plans, keep those plans up to date. And DR is more than just data backup and data replication: You've got to think about how you restore the applications themselves.

And then the piece that people often forget is people and communications. If something actually hits that remote site, it's probably not a problem to restore the data and restore the applications, but you've got to figure out a way to get those people back to work. Are they going to show up at an alternate location? Are you going to assume that people are going to work from home with SSL and VPN technologies?

You also need a way to do emergency communication. How do you blast out information to tell people, "Don't come to work, go here instead, this is when we expect you back at work"? And you also want two-way

↘ EDITOR'S LETTER

↘ CREATING A BRANCH OFFICE DR PLAN

↘ 5 WAYS TO SAVE ON BACKUP & RECOVERY

↘ CASE STUDY: 4 SITES, 5 LAYERS OF REDUNDANCY

↘ FLEXIBILITY, COST-EFFECTIVENESS WITH DUAL SANS

↘ IN HURRICANE ZONE, A MOVE TO MANAGED BACKUP

↘ A CIO'S ADVICE FOR REMOTE-SITE DR

communication to make sure everyone is OK, and you also want their updated contact information.

What critical steps are midmarket CIOs taking to incorporate their remote offices or branch offices into their DR strategies?

It's always helpful to step back and do a business impact analysis. In IT, we tend to focus on individual applications, and we lose sight of the business process. So if you focus more on enabling the business and enabling certain business processes, like "What is everything I need for order to cash, financial accounting and reporting, supply chain?" it gives you much broader perspective as to all the resources [you'll need]. And resources could be people, they could be physical assets, it could be IT assets.

I do think from a technology perspective, it makes a lot of sense to consolidate remote office backup, recovery and DR to some sort of centralized model; that gives you the insight as to what's actually happening there.

From the plan perspective, a lot of people are deploying resources so that they can share plans globally. Some companies are choosing to deploy software that will actually help you create and manage plans online. It's also helpful to have all your plans in one central repository that everyone can see.

How much should a midmarket CIO plan on spending when it comes to creating, maintaining, testing and updating DR strategies for remote and branch offices?

Some of these backup services are actually pretty inexpensive. They can be just a few dollars per gig, per server, per month, and that will actually give you data protection. One way to determine how much you should spend is to take more of a risk assessment approach, which is you look at the remote office and you do a risk assessment: What are the threats that we're expecting—power failures, natural disasters like hurricanes? You assign a probability to it, you determine the impact of the actual threat scenario, you annualize it, and that's basically how much you should spend on disaster recovery for that particular location.

How can you optimize your systems and connections for your remote and branch offices for a good DR foundation? And if you don't have an IT person on-site, how do you enforce these backup processes?

A lot of companies are consolidating infrastructure from remote offices entirely. So if you're used to having standalone file servers, app servers, some local storage, [you] completely eliminate that IT infrastructure, placing it all at the corporate data center and potentially using a WAN acceleration technology to facilitate better performance and access to your data and applications over the WAN. That eliminates the need to do any kind of [remote] backup at all, because everyone is just accessing their in-

(Continued on page 6)

↘ EDITOR'S LETTER

↘ CREATING A BRANCH OFFICE DR PLAN

↘ 5 WAYS TO SAVE ON BACKUP & RECOVERY

↘ CASE STUDY: 4 SITES, 5 LAYERS OF REDUNDANCY

↘ FLEXIBILITY, COST-EFFECTIVENESS WITH DUAL SANS

↘ IN HURRICANE ZONE, A MOVE TO MANAGED BACKUP

↘ A CIO'S ADVICE FOR REMOTE-SITE DR

Five Ways to Save on Backup and Recovery

WHEN ASKED TO name the toughest ongoing challenge in disaster recovery (DR) and business continuity (BC) planning, the majority of midsized organizations say it is inadequate funding. Here are five elements that can save your organization money:

1. Server Consolidation

Having fewer systems means there is less to recover in an emergency. "If you can consolidate your systems into a more fault-tolerant configuration, you have reduced your risk footprint dramatically," says Jim Copenhaver, a certified business continuity professional at Key Results Management Inc. in Atlanta. Consolidation saves on operational overhead, including personnel, redundant software licenses and patch management. HVAC, power consumption and network capacity costs also shrink.

2. A Technical Refresh

Older systems and tape drives incur maintenance costs that never decline. By performing a technical refresh, you can usually eliminate maintenance costs for three years. A good business case will show upper management that a capital expenditure spread out over three years will be revenue-neutral or even represent a savings.

3. A Tiered Recovery Architecture

Some backup processes, such as synchronous replication, are very sophisticated and expensive. They assure both minimal data loss and the fastest recovery time, but not all business systems deserve that kind of treatment. Gartner Inc. analyst Dave Russell advises that you design a tiered recovery architecture based on the mission criticality of each business system. These generally include real-time replication, snapshot replication, disk-based backup and tape-based backup.

By using less costly backup and recovery for lower-tiered business systems, you'll see substantial savings.

4. Negotiation

As you evaluate the recovery point objectives and recovery time objectives for different systems, Russell says, be prepared to negotiate with business process and applications owners because there are tradeoffs between risks and costs. In some cases, business owners may accept more risk for lower cost (which can mean slower recovery).

5. Competitive Friction

Gartner believes multiple vendors will soon offer layered recovery and unified management BC solutions. Now is the time to send out requests for proposals and review the DR and BC products you are running. Gartner recommends that you look for opportunities to leverage the competitive market, including switching to a new vendor to obtain a better deal. —LINDA TUCCI

(Continued from page 4)

ormation directly from the corporate data center.

But you still have to figure out how to back up PCs because you're not going to eliminate PCs. One way is backup software as a service. You could just say, "We're going to pay somebody a subscription fee, and they're going to back up our PCs and servers for us." Which is great—you don't have to deploy any infrastructure; you don't have to deploy any software. It's automatically off-site; they encrypt it for you.

The downside with backup software as a service, though, is restore. If you want to restore an individual file, no problem. If you need to restore, say, more than like 15 to 20 gigs of data, that becomes a problem over the Internet. So they'll actually restore your data to some sort of removable media and ship it to you. So you're looking at a recovery time objective of 24 hours.

Another way to do it is by eliminating tape and deploying some sort of disk appliance, where you back up locally to disk and you do a secondary replication or a vault of the data back to the corporate data center. There are at least three to four ways to consolidate it, but that's the basic theme: consolidation. Basically eliminating the need for any kind of local IT staff to actually have to manage the backup process, providing the visibility and manageability back to corporate IT.

What are some of the latest technologies available for these disaster recovery efforts that you've found in some of your research?

I do like the online services quite a bit. Now what they're actually doing with virtual technology is, they have copies of your system images and they'll either a., host you in a virtual environment if you need to fail over to them; or b., they'll restore your images, restore your data and quick-ship your servers to you. I think these online services hold a lot of potential for the remote offices.

If you want to keep it in-house, I think technologies like deduplication are making a big difference because if you can back up locally to an appliance and you still have immediate access to your data for restores, that's great. But then when you need to vault that information back to corporate, because the data is deduplicated, you're only sending unique data segments back to corporate. That means you don't need a lot of bandwidth between the sites in order to facilitate that. You can get away with just having T1 connections in between you and corporate. So that helps quite a bit as well.

[In summary], I think that anything online or in the cloud or virtual is huge. I think anything, either in software or in the appliance itself, that deduplicates the data to disk and then lets you replicate it remotely is also a big help as well. ■

KRISTEN CARETTA is associate editor for SearchCIO-Midmarket.com. Follow her on Twitter at @kcaretta or write to her at kcaretta@techtarget.com.

OPEN DAILY

CASE STUDY

Four Sites, Five Layers of Redundancy

CIO: Centralized data centers with plenty of backup assure electronic health records will be available for cancer center patients, no matter which facility they visit. **BY LINDA TUCCI**

→ **FOR SOME ORGANIZATIONS,** it takes an act of God to get serious about a disaster recovery plan for remote offices and branch offices. For Cancer Treatment Centers of America (CTCA), the organization's mission to treat patients like family members was more than enough motivation to make sure IT did it right, says CIO Chad Eckes. The proximate cause was a move from paper to electronic health records.

"Our promise to the patients was that we could ensure all of the appropriate documentation for their care was available as they moved through our very complex and very speedy system of treatment," says Eckes, who was recruited in December 2005 to spearhead the digital makeover at the for-profit CTCA, which has hospitals in suburban Chicago; Philadelphia; Tulsa, Okla.; and suburban Phoenix.

CTCA is what is sometimes called destination medicine: The average patient travels 500 miles to CTCA. He or she might receive treatment at multiple departments within a hospital or even receive care at more than one CTCA center, Eckes says. "The paper world couldn't keep up with movement of the patient," he says.

Cancer Treatment Centers of America has built in four layers of redundancy for its systems data, plus a fifth layer in the event of a worst-case scenario.

Going paperless, however, posed considerable risk. The electronic health records system could not go down. Electronic medical records needed to be reliably and securely managed, readily accessible for input

↘
EDITOR'S LETTER

↘
CREATING A BRANCH OFFICE DR PLAN

↘
5 WAYS TO SAVE ON BACKUP & RECOVERY

↘
CASE STUDY: 4 SITES, 5 LAYERS OF REDUNDANCY

↘
FLEXIBILITY, COST-EFFECTIVENESS WITH DUAL SANS

↘
IN HURRICANE ZONE, A MOVE TO MANAGED BACKUP

↘
A CIO'S ADVICE FOR REMOTE-SITE DR

and output of information and connected to the hospital's medical equipment.

"Those reasons are why we started going down the path of building a highly redundant infrastructure that was focused on disaster recovery," Eckes says.

REDUNDANCY AROUND THE CENTRALIZED DATA CENTERS

CTCA needed to have centralized data centers because its widely dispersed hospitals share electronic health records. But that also increases risk. "If an application goes down, that not only impacts the service offering at one hospital but across our four facilities," Eckes says.

Thus CTCA has built in four layers of redundancy for its systems data, plus a fifth layer in the event of a worst-case scenario:

- Each production system is clustered, so if one part of a cluster fails, the systems remain up and running.

- Every piece of data from all sites is immediately mirrored to a second data center, so in the event of an outage, CTCA can shift processing to the redundant center with no data loss. The CTCA located its second center 59 miles from its primary center in Schaumburg, Ill., a strategic decision based on the speed of data transmission. "We chose to have it this close because we couldn't replicate without it being this close. Information can only travel so fast over the lines."

- Backups are stored to disk. "Disk is very fast to restore off of, and we have that immediately available in our data center. We keep seven days' worth of backups on disk." CTCA backs up approximately 4 terabytes nightly.

- Standard tape backups are stored off-site in a vault facility in downtown Chicago. "We can't keep the disk backup as long as we want to, from a cost standpoint. It wouldn't be prudent. We also want to protect against a situation where both data centers go down."

- Data is in PDF format. In the event that all other redundancies fail, CTCA "has written a massive dump of data that goes out to all the individual sites." The data, which includes all vital patient information needed for care, is pulled every four hours and stored in PDF format on a server in each of the hospitals. "In the worst-case scenario, folks at that hospital

> **"If an application goes down, that not only impacts the service offering at one hospital but across our four facilities."**
>
> **—CHAD ECKES,** CIO, Cancer Treatment Centers of America

(Continued on page 11)

• Flexible, Cost Effective: Dual SANs, 100 MB Line

COMPANY: Arnold Worldwide Partners
INDUSTRY: Advertising
OFFICES: Boston; New York; Washington, D.C.
EMPLOYEES: 650
IT STAFF: 12 people
DR SOLUTION: Virtualization, dual SANs, 100 MB Ethernet over Sonet line

When Greg Folsom, senior vice president of IT at Arnold Worldwide Partners, a $100 million advertising firm in Boston, decided to upgrade the firm's DR infrastructure a couple of years ago, he combined a server virtualization effort with a virtualized storage area network (SAN). The result: Redundant data and a data pipe fat enough to route the firm's New York office through the Boston data center to the Internet—a dual use that makes it cost effective.

Folsom consolidated 45 servers in the Boston data center to four physical servers, using VMware ESX server software. The servers in New York are also virtualized. He installed a Compellent Storage Center SAN in Boston and a second Compellent SAN at the New York office. The Boston data is mirrored in New York and vice versa (asynchronous replication over IP) so he can bring up his Boston office in New York automatically or manually.

"I can figure out if this is a real disaster and want to bring up the machine in New York and then have to deal with bringing the data back to Boston, or if it makes sense to get the piece of hardware fixed and have the virtual machines moved to other Boston servers," he says. The Data Instant Replay (snapshots) can instantly restore a database containing metadata for nearly all of the agency's creative work.

He kept the tape backups Arnold relied on before, but now he also uses disk-to-disk backup and disk data deduplication.

Paul Clifford, founder of Davenport Group, a SAN integrator and Compellent partner, is a big fan of employing virtualization in the service of disaster recovery. "I think where most CIOs make their mistakes is that they really don't build a flexible plan. They build a plan 'to bring it up' if something goes wrong. The problem is that you cannot foresee all of the things that can go wrong."

In an ideal world, Folsom says, Boston, New York and D.C. would be replicating data amongst themselves. But his setup is still paying dividends.

"By day, we utilize the DR line for our employees in the [New York] DR site to come across to my network and get out to the Web and come through some security devices I have here in Boston, so I do not need to duplicate devices in their office," he says. The 100 MB line, Verizon's Ethernet over Sonet, provides "enough bandwidth to support the replication and normal business use," he says.—L.T.

↘ EDITOR'S LETTER

↘ CREATING A BRANCH OFFICE DR PLAN

↘ 5 WAYS TO SAVE ON BACKUP & RECOVERY

↘ CASE STUDY: 4 SITES, 5 LAYERS OF REDUNDANCY

↘ FLEXIBILITY, COST-EFFECTIVENESS WITH DUAL SANS

↘ IN HURRICANE ZONE, A MOVE TO MANAGED BACKUP

↘ A CIO'S ADVICE FOR REMOTE-SITE DR

(Continued from page 9)

can go to the server, print it off and be taking care of our patients safely."

The upshot is that if CTCA loses its main data center today, every system can be up and running within two hours; real-time replication guarantees zero data loss, Eckes says.

TAKING CONTROL OF THE UNCONTROLLABLE

But probably the toughest aspect of building the infrastructure to fully support going paperless was achieving network redundancy, the rung of disaster recovery that is not fully under one's control, Eckes says. The easy part was building high redundancy into the LANs at CTCA's facilities. Designing a structure at the metropolitan level and the wide area network level (WAN) proved more difficult.

"What we did—and we're told we have one of the most complex designs in greater Chicagoland—was to design two full-production, wide area network WANs," Eckes says. One WAN is with AT&T and one is with Qwest. The WANs, which transmit 20 megabytes per second, run synchronously and "are sized at a point that allows us to run on either/or and still have plenty of bandwidth to run both of our facilities," he says. Eckes also negotiated with the two telecom providers to make sure the CTCA networks are on independent fiber, to prevent the possibility of a single point of failure.

THE MISSION DICTATES THE DR PLAN

Eckes runs IT with a team of 84 people, and just as important as the nuts and bolts of disaster recovery is aligning the plan with CTCA's mission.

The upshot is that if Cancer Treatment Centers of America loses its main data center today, every system can be up and running within two hours. Plus, real-time replication guarantees zero data loss.

"What that translates to, from an IT perspective, is the question I constantly ask my team: 'If your mother or father were being treated here, hooked up to medical equipment that is connected to our EHR, how redundant would you want this system?'

"That is what drove our goal, which is 100% system uptime," he says, acknowledging that many IT people would dismiss that as impossible. "But why would you target anything less? We'll keep on chasing the tail of redundancy until we achieve that standard." ■

LINDA TUCCI is a senior news writer for SearchCIO.com and SearchCIO-Midmarket.com. Write to her at ltucci@techtarget.com.

Overland
STORAGE®

The Quest for Affordable Disaster Recovery is a Snap

The Overland Storage© Snap Server© delivers simple and affordable disaster recovery solutions

Whether you are a remote office or retail location, business critical data must be protected against any disaster—small or large, man-made or natural—at all times. Let Overland Storage guide you in your quest for a disaster recovery solution that is simple to manage and affordable to own, with the Snap Server family of NAS storage servers.

Snap Server combines powerful software applications and hardware configurations to deliver:

- Disaster Recovery and and remote office backup consolidation for SMB, SME and distributed enterprises
- A new level of affordability for Enterprise data mobility and management
- Cross-platform data replication between Overland's NAS Snap Server appliances, and Windows, Linux and UNIX Servers
- Data movement without disruption to end-users or applications
- Integrated tiered security with encryption, authentication and certified delivery

For more information on discovering the right disaster recovery solution, visit our microsite at:

www.overlandstorage.com/Quest

www.overlandstorage.com/Quest

Overland
STORAGE®

In Hurricane Zone, a Move to Managed Backup and Recovery

The move from tape to disk-based replication continues, as does the demand for online backup and DR services. Just ask the CIO of a $200M nonprofit in hurricane-prone Houston. **BY LINDA TUCCI**

→ **TOM COMELLA, CIO** of human services provider Neighborhood Centers Inc., pays roughly $1,500 a month to IBM to protect his organization's data with a managed backup and recovery service. A storage device located in the nonprofit's Houston headquarters collects the approximately 275 GB of data from 13 servers spread over seven sites, encrypts it and sends it to an IBM data center 1,200 miles away in Raleigh, N.C.

"Quite honestly, it is not a big ROI. In fact, I wouldn't even call it an ROI. We did this because it is a business decision. We have to protect our data," says Comella, who also serves as vice president of capital projects. In hurricane-prone Houston, the result is a disaster recovery process for pretty much any kind of weather.

The strategy reflects two trends in backup and recovery: the inexorable movement from tape to disk-based backup and the growing acceptance of using outside providers and the Internet for data protection.

Dave Russell, a research vice president at Gartner Inc. who specializes in storage management software, has seen the percentage of enterprises backing up directly to tape drop from 63% to 34% over the past four years. "That is a phenomenal shift," he says, especially in a discipline that by its nature is conservative. "Backup and disaster recovery have to be risk-averse."

The low cost of tape continues to make it attractive for long-term storage. Recent Gartner research showed that just more than half of enterprises—52%—use disk to disk to tape, Russell says, a reflection of the "layered approach" organizations are taking to storage backup and archiving.

Interest in managed backup and recovery services shows a similar trajectory, says Gartner principal analyst Adam Couture, who covers storage services at the Stamford, Conn.-based

↘
EDITOR'S LETTER

↘
CREATING A BRANCH OFFICE DR PLAN

↘
5 WAYS TO SAVE ON BACKUP & RECOVERY

↘
CASE STUDY: 4 SITES, 5 LAYERS OF REDUNDANCY

↘
FLEXIBILITY, COST-EFFECTIVENESS WITH DUAL SANS

↘
IN HURRICANE ZONE, A MOVE TO MANAGED BACKUP

↘
A CIO'S ADVICE FOR REMOTE-SITE DR

consultancy. A research study last fall showed that half of North American users were either currently using (21%) or considering using (29%) managed backup services, Couture says. Another 18% are no longer using these services and 32% have no interest whatsoever. A few years ago, the resistance was near 70%, he says. "Barriers are coming down."

A DRAW FOR SMBS

Managed backup and recovery services are particularly attractive for small and medium-sized businesses and for enterprises with remote locations, Couture says. "Maybe you don't have the staff to do it, maybe you've got high turnover." Backups are relegated to more junior people, if you do have an IT staff, or the night clerk, he says, recounting his recent arrival at a hotel in the wee hours and having the desk bell answered by a receptionist holding a tape. "These services just make sure backups happen and you can recover your data."

Having an appliance at the local site—a feature not offered by all providers—gives the ability to back up and restore data at land speed, instead of over the Internet, Couture says. A second copy is stored far away. Vendors like IBM have realized that they can turn their off-site storage services into disaster recovery services by adding a recovery option. And just recently, the SunGard Availability Services unit of SunGard Data Systems Inc. announced Secure2Disk, a new disk-based, online backup and recovery service that also offers an on-premise appliance.

JETTISONING TAPE BACKUP

Automating data backup, getting it out of harm's way and being able to retrieve it quickly are mission-critical tasks for Neighborhood Centers. With more than $180 million in annual revenue and 800 employees, the nonprofit offers "cradle to grave" services, from Head Start programs to senior citizen centers. Hundreds of thousands of people depend on its programs. The organization is also a recipient of Gulf Coast Ike Relief Fund grants and increasingly acts as a first-line responder in crisis situations. An IT staff of 12 manages 650 computers.

"My systems have to be secure and ready to go up," Comella says.

Moreover, data protection is good business strategy, he adds. "We respond to RFPs like any other company does. If I can say my data is secure and safe, it's a strategic initiative for me."

When Comella arrived at Neighborhood Centers four years ago, the organization was backing up data to tapes at some 20 locations, then "playing a shell game" of moving the tapes from building to building for storage. That strategy might suffice for some crises, but it was not a tenable disaster recovery plan for a geography that routinely faces major hurricanes (Rita, Ike) and took in more than 400,000 hurricane victims after Katrina. In fact, when Rita threatened,

↘ EDITOR'S LETTER

↘ CREATING A BRANCH OFFICE DR PLAN

↘ 5 WAYS TO SAVE ON BACKUP & RECOVERY

↘ CASE STUDY: 4 SITES, 5 LAYERS OF REDUNDANCY

↘ FLEXIBILITY, COST-EFFECTIVENESS WITH DUAL SANS

↘ IN HURRICANE ZONE, A MOVE TO MANAGED BACKUP

↘ A CIO'S ADVICE FOR REMOTE-SITE DR

Comella's director of IT took a set of master tapes with him on his way out of town.

"I did not feel real comfortable with that," Comella says. Aside from the obvious security risks in transit, tapes are susceptible to contamination. "I've been bitten in the past where I went to restore stuff from tape and the tape didn't work for whatever reason."

When he began looking for a way to provide better disaster recovery for his distributed computing environment, he had an IT department of six people and no one dedicated to tape backup and recovery. Data was growing at 20% per year. He wanted to automate data backup from PCs and servers, and storage of that data offsite.

IBM's managed, on-demand backup service, which is priced per gigabyte of data, is based on technology developed by Arsenal Digital Solutions, which IBM acquired in 2008. Comella says he likes that the solution provides fast data backup and fast restoration. The organization's most recent data sits on the local appliance at its headquarters. "We can get the stuff back fast if it's from the last couple of days." In case of a catastrophic event, IBM will ship a similar appliance with the backups overnight.

The data is duplicated and encrypted before being transmitted to Raleigh. Performance has not been an issue. Mail servers are backed up overnight, so they don't slow down users.

The snafus that have come up since implementing the solution—a corrupted file in a main financial system, for example—have been easily fixed, Comella says. "We've actually done live backups a few times and everything has worked as advertised." Once a week his director of IT checks to make sure the backups are working correctly.

> **"It is not a big ROI. In fact, I wouldn't even call it an ROI. We did this because it is a business decision. We have to protect our data."**
>
> **—TOM COMELLA,** CIO, Neighborhood Centers Inc.

The oft-cited risks associated with online backup and remote storage—that your company's top secrets are commingled with competitors'; that despite encryption, a provider can see your data; that the service will always be more expensive than making a tape yourself—don't keep Comella up at night.

"We've seen it work, we've seen restores happen. It's one less thing I have to worry about. I can move on to things that need my attention a lot more than backup and storage," he says. ■

LINDA TUCCI is a senior news writer for SearchCIO.com and SearchCIO-Midmarket.com. Write to her at ltucci@techtarget.com.

THE REAL NIEL

A CIO's Advice for Remote-Site DR

How to increase the chances that a remote site will recover from an outage. **BY NIEL NICKOLAISEN**

→ **SOME DAYS I** long to be the benevolent dictator of all of our IT. Sure, I am the leader of IT, but I am not in complete control. My control over IT decreases as we distribute IT to our remote sites. I can specify the equipment they use, but I can't control what they do with the equipment. I can define processes and practices for how our remote sites use IT, but I can't monitor what our remote sites actually do. This has implications for my remote-site disaster recovery and business continuity plans.

But it begins with the everyday. For example, an employee at one of our remote sites considers himself, erroneously, to be quite adept at IT. So, when the site needs IT support, the site does not call the service desk. Instead, employees call Carl. Carl does his magic and shuts down the site. Carl then calls the service desk so we can bail him out. Try as I might, I cannot get the remote site to call us first. But if I were really in control of IT, I would exercise my rights as a benevolent dictator and have Carl put in stocks.

Back to disaster recovery and business continuity, which are among my remote-site sore spots. Let's face it: With the trouble we have managing backup and restore at our primary data centers, our remote sites barely have a chance. So, we need to make the process as simple and straightforward as possible.

I start by really thinking through what remote-site systems and data the business absolutely, positively needs. That is where I focus my attention. I like to sort my systems and data into three broad categories—A, B and C:

- If A systems are down for a few minutes, the business is at risk.
- B systems can be down for a few hours before the business is at risk.
- C systems can be down for a long time before the business is at risk. (One time, one of our C systems

was down for six weeks before anyone outside IT noticed.)

I focus both my data center and remote-site disaster recovery and business continuity plans and tools on the A systems and data. Sorting our systems this way sometimes means that I don't need to worry about remote-site backup and recovery at all—and what is simpler than that?

If, after stratifying systems into A, B, and C categories I still need to provide disaster recovery and business continuity to remote sites, I turn my attention to instructions that are written well, simply and clearly. These cover backup and recovery procedures, how to communicate in the event of an event, what to tell customers, etc.

For our procedures, we first find a willing or unwilling person or team in IT to write the first draft. We include lots of pictures to accompany our well-, simply and clearly written procedures. We then have someone in IT try out the instructions to see if he can accomplish the task. Once we fill in any of the gaps that this first test revealed, we ask one of our end users to follow the instructions. With this done, we send out the instructions and then cross our fingers that nothing really goes wrong.

When we are feeling bold and brave, we have one of our remote sites test our procedures by simulating an event. Can people there get access to and install their data backups and get back in business? What happens if they lose network and Internet connectivity? Can they contact employees and customers if the phone system is out? With just a few scenarios, we can usually find and fix the holes we have in our processes. With the right attitude, these tests end up being somewhat entertaining—especially if you enjoy watching people wander around the neighborhood trying to remember the location of their safe gathering spot.

Sort, document and test. That is what I do to improve the chances my remote sites will recover from what can go wrong. Not quite the control of a benevolent dictator—but I will take what I can get. ■

NIEL NICKOLAISEN is CIO and vice president of strategic planning at Headwaters Inc. in South Jordan, Utah. Write to him at nnick@headwaters.com or editor@searchcio-midmarket.com.

CIO Decisions Ezine is produced by CIO/IT Strategy Media, © 2009 by TechTarget.
Managing Editor: **Jacqueline Biscobing**; Editorial Director: **Anne McCrory**; Designer: **Linda Koury**; Executive Editors: **Karen Guglielmo** and **Scot Petersen**; Associate Editors: **Kristen Caretta**, **Alexander B. Howard** and **Rachel Lebeaux**; Senior News Writers: **Christina Torode** and **Linda Tucci**; Contributing Writer: **Niel Nickolaisen**.
For sales inquiries, please contact **Stephanie Corby**, Senior Director of Product Management, scorby@techtarget.com (781) 657-1589.

CIO Decisions Business Staff
Senior Vice President and Group Publisher: **Andrew Briney**; Publisher, Sales: **Jillian Coffin**; Senior Director of Product Management: **Stephanie Corby**; Product Managers: **Kari Lindquist** and **Theron Shreve**; Marketing Manager: **Katie Graybeal**; Marketing Programs Associate: **Lee Tetreault**

RESOURCES FROM OUR SPONSOR

i365

A Seagate Company

- The Keys for Disaster Recovery Planning. Read this white paper and learn how to proactively prepare your organization.

- Best Practices for Data Protection for ROBOs (Remote Office, Branch Office)

- Best Ideas in Disaster Recovery. Three case studies of what they have done to solve their disaster recovery challenges.

About i365, A Seagate Company

i365, A Seagate Company, provides proven solutions for the protection, retention, and discovery of electronic information. Trusted by over 22,000 customers, our innovative technologies combined with flexible deployment options form solutions to solve organizations' most rigorous compliance and data management problems. Our solutions address the complexity of explosive data growth, the challenge of maintaining high availability of critical business systems, and the increasing demands of regulatory compliance and litigation. Our offerings include i365 EVault Data Protection software and SaaS for backup and recovery; i365 Retention Management solutions for data recovery, migration, restoration and data management solutions; i365 MetaLINCS E-Discovery solutions for first pass processing and advanced content analysis of electronic information; and i365 ProServ Professional Services for implementation, consulting, training, and risk assessment of the i365 portfolio.

RESOURCES FROM OUR SPONSOR

About Overland Storage