

# **Lessons Learned:**

## **Business Continuity and Disaster Recovery after the 2005 Hurricane Season**

Feb 2006  
CyrusOne, LLC.

**WHITE**  
paper

**Twenty-seven named storms. Three Category 5 hurricanes. Two hundred billion in damage from Katrina alone. 2005 slammed the Gulf Coast with the most destructive hurricane season in history, and the region's IT infrastructure felt the sting. With 2005 in mind, what can IT leaders do this year to minimize operational and financial risks?**

Across the globe last year, people watched in horror as the Gulf Coast withstood the most vicious tropical storm season in U.S. history. On the macro-level, the U.S. Gross Domestic Product (GDP) took a .4 percentage point hit in the second half of last year, as entire regions of the country not only incurred terrific losses but also paralyzed previously prolific economies. At the micro-level, businesses--some quite substantial--shuttered never to open again, gas prices spiked and many a fortune evaporated. And the personal effects of the storms received global attention.

Behind the scenes, IT leaders and staff worked miracles to keep companies enduring Katrina, Rita and Wilma up and running--or at least minimize loss. Many watched as business continuity and disaster recovery materialized from hazy concepts to hard reality. And for business leaders whose bailiwicks fall outside of IT, those barely-remembered pleas for contingency-related IT expenditures suddenly came back to mind.

So as we move in 2006, what lessons are we taking with us into the upcoming hurricane season that will enable IT leaders from small businesses and Fortune 500 companies alike to escape the most egregious pitfalls of the 2005 hurricane season? Tactically, there are hundreds if not thousands. But strategically, six especially critical lessons emerged from the storm season:

1. Understand the stakes
2. Avoid the technology trap
3. Maintain executive buy-in
4. Keep plans current
5. Move sooner rather than later
6. Know the drill

## **Lesson 1: Understand the Stakes**

*How much does downtime cost you? Specifically?*

The answer is different for every enterprise, but one thing many an IT leader found out during the 2005 hurricane season is that simply knowing the cost of downtime is critical. For every hour, for every day, for every week a particular application or system is down there is a financial impact. Know the numbers. "If people can understand what the cost of downtime is," notes CyrusOne Technology VP Dan Vazquez, "then they have the information and motivation they need to move forward and plan accordingly beforehand. Many times people

don't understand the costs associated with downtime so they have a tough time getting their hands around business continuity and disaster recovery."

When it comes to your company's valuable data and functional applications, the whole is greater than the sum of the parts. Having a spreadsheet outlaying the specific cost of IT application, internet and network downtime is the only way of knowing whether you're truly investing in a protection of your company's operation or simply being scared into overspending following a major disaster. When you have the numbers, you know where you stand. Don't have time to figure it out? Hire a consultant to do it for you. Just get the numbers.

## **Lesson 2: Avoid the Technology Trap**

*Don't forget "people infrastructure"*

Servers. Back-up tapes. Generators. These are the tangibles that initially come to mind when one considers disaster recovery and business continuity preparedness. But there are two sides to the coin: the technology that's the obvious component, and the second one--people. Dohsung Yum is Director, IT Enterprise for knowledge-based service assurance provider NetIQ: "When Tropical Storm Alison hit, we had the technology covered: the financial systems, CRM, file servers--we were fine. But that wasn't quite the case on the people side. The building we were in wouldn't let us back in without power. No elevators. No phones for tech support or sales to use." Yum made alternative arrangements on the spot for some "people infrastructure" to get a temporary shop up and running for critical personnel, then modified his contingency plan. When Rita loomed in 2005, hardened offsite office space was in place right down to fresh coffee for the critical personnel.

And outside of human and technical infrastructure, IT leaders must also remember that disasters affect HR availability and reliability. During the 2005 hurricanes, many were not willing to tackle work issues in lieu of turning their attentions toward their families' safety--a perfectly natural response. "Leading up to Rita, we flew a small group of order management personnel from our Houston data center out to San Jose, California facility, just in case," notes NetIQ's Dohsung Yum. "It was hard to find people to go. They were concerned about their families, boarding up their windows, traveling. They didn't want to be far from home." NetIQ has addressed the issue by replacing their San Jose facility with one that's local, a move that was already underway for economic purposes.

But people's natural desire to be with their families means resources can evaporate or muddle in terms of which responsibilities fall under whose aegis. Assign critical roles to those who are comfortable with being away from their families, or to make arrangements for the families of critical staffers' safety in advance which so they can focus on their jobs comfortably. Everybody wants their families to be physically safe and comfortable, but we also need healthy companies to come back to for our families' financial wellbeing.

## **Lesson 3: Maintain Executive Buy-in**

*Keep executive buy-in all year*

In the weeks leading up to and following a hurricane, C-level executives, board members and other stakeholder hang on the every word of those responsible for disaster recovery and business continuity. Unfortunately, that attention is short-lived. Hurricane season passes. New crises emerge. These challenges become yesterday's headline. One lesson 2005's storm season teaches us is that it's the CIO's role to keep the momentum of contingency support going all year long. Armed with hard numbers, potential risks and a solid case for why executives should care, this is critical for getting the resources you need to succeed. And since you will be the ones feeling the heat if those contingencies fail, it's in your own best interest.

## **Lesson 4: Keep Plans Current**

*On outdated plan is a useless plan*

Another unfortunate trend brought forth by the storm was a sudden realization that many business continuity and disaster recovery plans were out of date. These plans have to live and breathe. Don't make the mistake of drafting a brilliant plan and then shelving it as your organization lives on to make operational and environment changes, pursue new corporate objectives or access a different portfolio of IT resources. You should, with every operational change, ask yourself: "How does this affect my disaster recovery plan? How does this affect potential downtime?" It sounds obvious, but as any venture capitalist will tell you, ideas are easy--it's the execution that matters.

## **Lesson 5: Move Sooner, not Later**

*You never know when disaster will strike*

Mark Groeschel doesn't like to take risks. An ex-MP, his military training and experience can be seen in the way he dispatches his affairs as IT Systems Support/Crisis Permanence at one of the world's largest integrated oil and gas companies. It's building demands uptime to support gas trading activities during business hours, so when the rare appearance of a single snowflake caused a power transformer to fail in his building he took immediate action. Fortunately the incident occurred on Christmas Eve when the trading floor was closed (This was the first time in recorded history it snowed in Houston on this day; the temperature there only drops below freezing once every five or so years.) Groeschel immediately drew up a plan that would lessen the risk of facility downtime, which included outsourcing core IT infrastructure to a power-redundant facility. But before the system migration was 100 percent complete, he had the unfortunate bad luck to find Rita upon them.

“We had just finished negotiations to outsource when Rita hit. So five days prior to landfall, I had to come up with a contingency plan which involved transferring 10 people to our London office. Getting data to the London office was hard. Fortunately, since we were in full disaster recovery mode and Houston didn’t get hit the way everyone thought it would so we were up and running the following Monday and it turned out to be a pretty good week for us because all of the other trading floors were still recovering.” This year, since Groeschel’s offsite data center and new business continuity plan will be in place, both power redundancy and his difficulty getting data to the London location will be ameliorated. “It would have been a much smoother road, though,” he says, “if we had been fully operational at our local data center when it hit. We’re hoping we don’t get anything as bad as we did last year, but it looks like we may it just as bad or worse.”

## **Lesson 6: Know the drill**

*If you fail to plan...*

Power. Connectivity. Employee and partner communication. PR. Before you need to deploy your business continuity or disaster recovery plan, have processes in place for all fundamental infrastructure, back-office and communication needs. Whether you’re dealing in facility design, roles and responsibilities or operational planning--the simple exercise of holding all phone calls, clearing your desk and laying all the facts out in front of you for a rigorous series of “what if questioning” has true power.

And you may not have to start from scratch. “In 2005, some companies were more prepared than others because of compliance demands,” notes CyrusOne’s Vazquez. Those companies who were forced to make investments in compliance for regulations like The US Public Company Accounting Reform and Investor Protection Act of 2002 (Sarbanes-Oxley) survived better than smaller enterprises that failed to see continuity expenditures as the cost of doing business. So some of those processes can be used as a template, though it’s by no means comprehensive. Disaster recovery is not technically a mandatory part of SOX regulation, though it is a practical component of sound IT stewardship. After all, if a company loses its financial information it’s in for big trouble.

## **2006 Hurricane Season: More of the Same?**

*It depends on who you ask*

ABC reports that: “William Gray of Colorado State University predicted 17 named storms in 2006, almost double the long-term average, and said nine of them could become hurricanes five of them major hurricanes, with winds of at least 111 mph.” Some climatologists believe the recent activity represents normal fluctuations between high and low intensity seasons though the lack of historical data and differing opinions make this reasoning far from definitive. In a tactical

sense, winds speeds, warm water and geothermal conditions all contributed to the year's activity. One thing is for sure, however, boardrooms not just around the Gulf Coast but around the world will be paying attention to the hurricane hype that's bound to be especially heavy in 2006, and wondering: "Are we ready?"

# # #

### **About CyrusOne**

CyrusOne is a leader in IT infrastructure outsourcing, providing managed hosting, colocation and managed IT services. We help businesses optimize returns on technology investment while ensuring application availability, data security and superior network performance. We were the first business of our kind to offer a 100 percent availability guarantee backed by the industry's leading Service Level Agreement. For more information, visit [www.cyrusone.com](http://www.cyrusone.com) or call 1-866-297-8766.