1 of 1 DOCUMENT

The Chronicle of Higher Education

December 9, 2005 Friday

SECTION: INFORMATION TECHNOLOGY; Pg. 200 Vol. 52 No. 16

LENGTH: 2185 words

HEADLINE: A Look Back at a Disaster Plan: What Went Wrong and Right

BODY:

In the aftermath of Hurricane Katrina, universities in the gulf were devastated. As hard hit as their physical plants was the information technology that touches almost every aspect of their operations. Tulane University had a disaster plan. Some of it worked. Some of it didn't. John Lawson, vice president for information technology and chief information officer at Tulane, talked about that.

Robert Burns got it right in his poem about a mouse whose nest was destroyed
by a plow the best-laid plans sometimes don't go where we expect. That's why I
think of my story as "The True Confessions of John Lawson."

Consider the four P's and an A for disaster recovery: planning, preparation, assessment, process, and people.

Planning: Tulane did a lot of planning for hurricanes. We didn't do a lot for earthquakes, but we did a lot for hurricanes. Our disaster plans were based upon time, location, and intensitythat is, the hours until a storm's projected landfall, its location in the gulf, and its projected strength. Student safety was our first concern. For information technology, our plan said: If it's a Category 1 to Category 3 hurricane, we would complete backing up all systems
telephone and network, as well as applications 24 hours out of landfall. We would have a skeleton crew at key locations to keep systems up. We would activate our emergency Web site to communicate to students updates on what the university was doing and how close the storm was, with a link on our home page.

For Category 4 to Category 5: We would complete our backups 36 hours out. The president would have the option of ordering a complete evacuation. If the complete evacuation were ordered, we would turn our system off in the data center. We would move our DNS (Domain Name Server) records, which provide all the Internet addresses in the university, to an alternate site that we had arranged with the University of Texas at Dallas. We would activate our emergency Web site, and our regular university site would go dark.

We were to go dark because we would be evacuating personnel. We could keep systems up remotely, but we didn't plan to do that, simply because we could never know when the power would go off. If we started losing air-conditioning and the network was down, then we would burn up machines, and we'd have another disaster. That is one of those policies we will re-evaluate: whether we go dark.

True confessions: Tulane did not have a formal disaster-recovery plan for replacement of machines with any outside vendor or institution. That was a cabinet-level decision, made during times of fiscal stress. We had just shifted to a decentralized system for fiscal management, so IT was a shared resource.
When I presented the plan for off-site disaster recovery, it was for $300,000 a year or so. We decided that we could not ask the deans to pay for that because they were already upset about how much technology was costing them, what they were getting for it, and whether it was giving them value. So it was a conscious decision, knowing there were risks.

Advice to presidents: Listen to the chief information officer. That's the big
thing about a disaster it's a disaster. Bad things will happen.

Advice to CIO's: Don't take no for an answer. Somehow you've got to persuade administrators to spend the money on disaster-recovery plans. Some colleges have done it very well. They have their own backup sites. Other colleges have signed agreements with vendors. Others have made agreements with other institutions.
But do something.

Preparation: Be prepared to follow the plan and take criticism. People are going to second-guess you. Make sure your emergency-operation center is stocked appropriately for the number of people who are going to be in it, for days upon end.

Test your communications plan and have a backup.

Make sure you're as prepared as possible for your postdisaster activity. That means you need to know where your people are. You need to know how they can get back, and you need to have a place for them to get back to.

You also need a business-continuity plan for your institution. You've got to think about how you are going to function if a disaster happens. How long can you go without printing transcripts, how long without sending paychecks out, how long without paying bills? How long can you tolerate not sending out accounts-receivable statements? You need to make those choices, so you'll know how much money you'll have to spend on disaster recovery.

True confessions: Our communications plan was not as robust as we needed. The telephone switch on our uptown campus lasted longer than anyone expected. We had a generator, we got fuel to it for a while, and it stayed up for a long time.
Our cellular communication went down faster than expected. I now carry a cellphone from one provider on one side of my belt and a phone from another on the other side. The lines were so clogged we had to keep trying different providers. We even had to get cellular phones with a different area code because the New Orleans code was completely plugged.

And people were too dispersed for postdisaster activity, which was exacerbated by the communications failure. We couldn't get hold of people to find out where they were. I had my director of administrative computing evacuating to one city; my director of networking, who was supposed to go with me, ended up in a different city because of traffic. We had people spread out all over.

We had dutifully made backups of all our data, had them all ready, had the pickup scheduled. When I evacuated, the tapes were sitting in their boxes ready to be picked up. If I could live that over, I'd be picking those tapes up myself. We had recently moved into a high-rise building downtown. It was leased space. Unknown to us, the building management closed it before the pickup could be made. The people came to get the tapes, and the building was locked. Our tapes were safe; they were on the 14th floor, in an interior hallway. We just couldn't get to them.

Advice to presidents: Finance the backup systems, and provide the funds to evacuate all your key personnel to one place. You'll have to talk to the lawyers about that because there are some liability issues if you're telling people they
have to go to a certain place and remember they're taking their families with
them but you've got to make sure that your key people are in position to help
you with determining what your future will be.

Advice to CIO's: Don't rely upon cellular and push-to-talk networks. Have an old-fashioned radio system for backup communications on campus. Educate your key personnel on text messaging. We couldn't make a voice phone call, but we could use text messaging on our phones, because that used so much less bandwidth.
Again, put your key personnel in one location, out of harm's way.

Assessment: You've got to take stock of the damage and how you'll recover from it. What's the situation going to be for housing your people? That's the major issue that we're dealing with right now. We want to open, but our people have to live somewhere. Do we buy apartment buildings? Do we rely upon the Federal Emergency Management Agency to bring trailers in?

You've also got to take stock of your human resourceswho's available and what 's their work capacity. Remember that damage isn't just physical. Some of those people are dealing with personal loss because they don't know where family members are, or they're dealing with the loss of their home.

Then take stock of outside resources. Who can help?

The big thing: Take control. As a president, as a CIO, you're in the best position to look out for your own institution. Don't rely upon FEMA. Don't rely upon the government. Don't rely upon the state. Take control of the situation.

Advice to presidents: Watch out for rumors. Be temperate in your reactions.
Verify before you comment.

Advice to CIO's: Frankly communicate the information-technology status to the leadership team. Now is not the time to waffle. Be realistic about what you can do and when you can do it.

Process: Let me list some points:

* Communicate, communicate, communicate. That is huge. Our president, Scott S. Cowen, has done a fantastic job making sure that people know what the situation is at Tulane. If you've followed our Web site, for a while it had daily updates. Now they're less frequent, but we're still trying to keep people aware of what's going on.

* Keep your public-relations people close. You'll need them. They will help you stay consistent with your message and provide insight for communicating with the wide variety of news-media inquiries you will receive.

* Use outside firms experienced in disaster recovery to jump-start the process. Get hold of them early, so that you're one of the first on their list. FEMA, the government, and your insurance company will respond but more
slowly than you expect.

* Prepare your board of trustees for the long haul. You've got a lot of things to take care of, and you can't be asking the board about every move you make. But you've got to prepare them for what it takes to recover.

* Think universitywide. The first step our president took was to disband the administrative cabinet.

My first reaction was, He disbanded the cabinet?

But what he really did was increase the size of the cabinet by bringing in key administrators and faculty members who could rise above divisions. Because we needed wise advice.

We also disbanded the decentralized-management concept. The deans had to understand: It's now Tulane University. Your money is our money, and we're going to help you recover, but we've all got to let go of our egos.

Under our old system, for accounts receivable, our controller had set up his own IT shop, and it did a great job. But guess what? When Katrina hit, those machines got flooded, and we couldn't recover them. There are just some things
that you need to have centralized control over so you have one point of failure or success.

* Be aware that your e-mail system is critical. After Katrina ours was brought online only for a limited subset of administrators and faculty and

staff members. That was our No. 1 internal complaint. The reason was that our e-mail system was in New Orleans, and our network was down. So we went to Yahoo. But we didn't have those backup tapes, so we didn't have a list of all our user names.

* Pay attention to your emergency Web site. When we first activated it, we were so frustrated because our vendor had made a change to virtual servers. The IP address for the site kept changing. We had to get hold of them to fix that.

* Realize that employee registration is important. You need to make sure that your employees can tell you where they are. It lets them know that you care, but it also lets you know where your resources are.

Advice to presidents: Don't wait on the technology folks, because they'll have their hands full. For call centers, we went out-side. Frequent Web updates,
the electronic chats we found a company that would help us on those.

Advice to CIO's: E-mail and the Web have become your lifeblood. Know their status at all times. Have a thick skin and a soft heart. You will be the hero and the goat, often at the same time. Don't be upset at the use of outside resources facilitate it. Don't be surprised when old vending partners disappoint you I can't tell you how frustrated I am with one of ours while
other partners support you in unexpected ways.

People: It's all about people. You've got to be sensitive to their needs, but you also have to be honest and forthcoming about the capacity of the institution to recover. Keep your cash flow in mind, obviously, because there are going to be many ways to spend money. But put people before invoices. Tulane did not miss a payroll. We were two days late on our first payroll after the storm because we had problems recovering damaged paychecks that were in the mail or the mailroom, and recovering the printer from campus. Of course, payroll runs on a printer that has a special security device on it, right? The disaster-recovery plan said that the payroll people would take that printer with them. Didn't happen.
Consider requiring direct deposit, or cash cards for those who don't want a checking account.

We did have to face the music. We stopped paying adjuncts on August 29. We stopped paying part-time faculty and staff members on September 30. Beginning November 1 we began using vacation and sick leave to help pay full-time faculty and staff members.

But it's all about people. I keep hearing in my mind a television interview with a New Orleans resident in the wake of Katrina. "I'm lost. That's all I had.
That's all I had," he said. "I'm lost." That's how a lot of our people felt.

We've got to help people like that man so affected by tragedy. But this is also about other people: They are our students. They are our prospective students. Tulane has been around for 161 years. We want to be around for quite a few more, and we will be. We're going to be there for those students because we are helping them prepare for the future. It's all about people.

LOAD-DATE: December 6, 2005