IT Disaster Recovery Near the World Trade Center

Following the September 11 terrorist attacks on the World Trade Center, nearby Pace University faced emergency conditions in implementing a disaster recovery plan

By Frank J. Monaco

“A great plan, vigorously executed, is better than a poor or incomplete plan, vigorously executed, and much better than a great plan, poorly executed, and much, much better than a poor or incomplete plan, poorly executed.”
—Anonymous U.S. Army Proverb

Business continuity planning, disaster recovery, and the Army concept “continuity of operations planning” have been on my mind for the past four years as I transitioned from the U.S. Army to the civilian world of higher education. Although my job responsibilities stayed much the same, acting as chief information officer for the United States Military Academy at West Point, New York, wasn’t exactly the same as being CIO at Pace University in New York City.

Charged with providing information technology services to more than 14,000 students and 2,500 staff and faculty, I was worried that at Pace we only had one of everything important. Sure, we backed up our systems and took the tapes off site on a regular basis. Still, whenever an outage occurred — especially a server crash or disruption of a backbone internal network or the Internet — students, faculty, staff, alumni, and the public were immediately affected, and teaching and learning were interrupted.

Pace University’s Division of Information Technology (DoIT) began taking steps about two years ago to minimize IT disruptions. Specifically, DoIT formed a committee to do something about these concerns, while interfacing with the university’s effort to build a comprehensive business continuity plan for areas other than IT. We consolidated mission-critical servers (including our Web pages, student information system, human resource system, financial system, e-mail system, library, and courseware systems) into a protected environment having a fire suppression system, an uninterruptible power supply with generator backup, and all-hours human oversight. We started to cluster our open systems mission-critical servers to get redundancy. We contracted for redundant backbone links. We occupied a single building on our Briarcliff Manor, New York, Westchester County Campus, making it Pace University’s Information Technology Facility. We purchased a disaster recovery template document from the Gartner Group and began the process of implementing the numerous suggestions and checklists contained therein. Sadly, the tragic events of September 11, 2001 interfered with the completion of our (and the university’s) disaster recovery planning. Without warning, we faced the emergency implementation of what plans we did have in response to the appalling destruction in our city.
from the WTC site, across the street from City Hall Park, making it the closest major university to the WTC. New Yorkers call this area “downtown.” We also have locations in “midtown” Manhattan and Westchester County: the Law School and Graduate Center in White Plains, New York; the main undergraduate campus in Pleasantville; and back-office operations and dorms, including IT, in Briarcliff Manor, which is about 40 miles from the downtown campus. At the time of the attacks, I was attending a meeting in midtown Manhattan that might well have been scheduled for the WTC location.

As part of the larger university response to this crisis, our president and executive council set up an emergency command center at our midtown campus and immediately dispatched our executive vice president for finance and administration to our downtown campus. Our main campus played an immediate role as well, when the debris cloud from the devastating WTC collapse traveled down the back streets, forcing people toward our main campus buildings. There they were assisted by our security professionals. The New York Police Department, Emergency Services, Port Authority Police, New York Fire Department, and National Guard set up triage, and later, staging areas, in our front lobby. We eventually had to evacuate the downtown New York City campus sites and dorms, sending students and staff to our Westchester locations.

**Infrastructure Destroyed**

The Verizon facility at 140 West Street, possibly the largest and most complex telecommunications facility in the world, was severely damaged by the destruction of World Trade Center Building #7. Although not directly targeted, the building suffered massive collateral damage. (See Figure 1.) Circuits (more than 300,000 voice grade and 3,500,000 data grade) and equipment began to fail the evening of the 11th, and power eventually went out in the entire area.

At midnight on the 11th, I was amazed when I finally walked outside our midtown location near Fifth Avenue en route to Grand Central Station. The city seemed deserted. I saw no people or moving vehicles in one of the all-hours busiest intersections in the world. In addition, United States Air Force fighter jets were flying combat air patrol high overhead. I will never forget that moment.

Early on the morning of the 12th, our Internet connectivity failed due to the Verizon facility’s damage — debris, soot, fire, and water had finally taken their toll. (See Figures 2 and 3.) Our internal network connecting all the campus sites (except for the destroyed WTC location) somehow survived. We used fiber distributed data interface (FDDI) for the backbone network. However, our Internet service provider (Applied Theory) stopped working because it rode Verizon on both primary and alternate routes. We were off the Internet! We also lost phone service to Manhattan, including cell phones for a short time because of antenna destruction and cell overuse.

**Picking up the Pieces**

Our chief technology officer literally picked up our mission-critical external servers and moved them to a disaster recovery site (Xand.Com, in Hawthorne, New York). Our Domain Name Service (DNS) administrator contacted the Internic (which handles DNS changes) and re-hosted our mission-critical external systems there. These systems stayed there for about one week. It took 24 hours for the new IP addresses to propagate, but once done, our Web pages and e-mail came back up on the Internet again.
It was extremely important to have Internet connection again because our downtown phones weren’t working either, meaning parents, students, and the public couldn’t contact our Manhattan campus sites. Because our Internet link to the disaster recovery site also wasn’t functional, our CTO devised an ingenious scheme to use dial-up networking to relay e-mail back and forth to our internal network. Once the Internet returned, we moved services from the disaster site back to our IT facility in Briarcliff Manor.

Believe it or not, we then got hit with the W32/Nimda@MM virus. Apparently, during our Internet outage, our virus signature files weren’t automatically updated. When the Internet came back up, infected e-mails had already arrived before the virus signature file updates. (Remember, we were relaying e-mail from the disaster recovery site.) We spent the first day back on the Internet cleaning up that mess.

Once we were allowed to reoccupy our main New York City campus, we obtained additional cell phones and published a previously well-protected cell phone list of the university administrators. We also used instant messaging, LAN fax, and e-mail to communicate with the NYC campus for almost 10 days, until we got land-line phones back.

During the university president’s daily crisis briefings, we actually used my old Army Readiness report formats to keep our staff and customers advised of our systems’ recovery. In the sample report shown in Figure 4, Red = No Functionality; Amber = Limited Functionality; Green = Normal Functionality; and ETR = Estimated Time to Repair. This approach worked extremely well, as — in my experience, anyway — informed customers are happy customers.

I should stress that restoring IT affected by the events of September 11 was only a very small part of the tremendous effort exerted by our president, executive staff, administrative staff, faculty, and students as we all started the long process of returning to some semblance of normalcy at Pace University. Our team came together for everything from convoying students on deserted downtown New York City streets to our Westchester campus sites, to installing multiple megawatt generators, printing and “snail” mailing thousands of letters, cleaning offices, and finding space and equipment for displaced staff and students. I am happy that IT — and all the hard-working people in DoIT — have and will continue to play an important role in this process.
Lessons Learned

As a result of the immediate consequences for Pace University of the September 11 attacks on the WTC, we got a first-hand look at what a university needs to recover from a disaster. The lessons we learned cover a wide range of topics, some totally unexpected.

- Have smart, energetic people working for you, especially your CTO and telecommunications director. At Pace University, these individuals were directly responsible for the vigorous execution of our less than great plan.
- Make certain that your ISP has diverse routing. That is, the primary and alternate routes should not go through the same phone company’s dial central office or major Internet point of presence facilities.
- Identify a disaster recovery (or application hosting) site completely independent of your campus sites, with multiple ISPs. Rent at least one rack there. Develop a good relationship with the people who work there.
- Ensure that this disaster recovery site hosts either your primary or secondary external DNS.
- Have a good relationship with your wireless cell phone service providers. We received free AT&T cell phones and service while our land lines were down, for example.
- Have strategic systems equipped with dial-up networking access. Also, have a few notebook computers with nonuniversity ISP access for loaners (say, 5 to 10 machines).
- Make certain that you have cable or satellite (preferred) TV access in all public gathering areas and potential crisis meeting places.
- Maintain an accurate cell-phone directory with university (and nonuniversity) owned cell phones.
- If your Internet link goes down, ensure that you obtain and distribute virus signature updates using dial-up networking before the Internet returns.
- Maintain alternate (that is, home) e-mail addresses for students, faculty, and staff. Also, prepare a well-advertised, nonuniversity hosted Web site (such as Yahoo Newsgroups) to get the word out in the event of a catastrophic Web page outage.
- Be ready to extract snail-mail rosters from your data warehouse for all conceivable university constituencies (for example, parents of Pace University’s New York City dorm students…)
- Have toll-free numbers you can immediately “call forward” (with in-house staff) to telephone banks for university hot lines. We used a bank of 11 phones, staffed at all hours for the first two weeks of the crisis.
- Be able to publish these toll-free numbers quickly via various media and the Web for wide distribution and access by interested parties.
- Be ready to staff the emergency phone lines heavily and nonstop during the first days following the crisis. The Pace University emergency information number received thousands of calls, handled by university staff and faculty who volunteered to serve as hot line operators.

For the September 11 disaster, I believe that we had in place an IT disaster recovery plan somewhere between great and poor or incomplete. Nevertheless, we did execute the plan vigorously, with notable success. I trust we will complete our disaster recovery plan and have a great plan ready, vigorously executed next time. Of course, we hope that there won’t be a next time, for any reason. Meanwhile, we continue to pray for the victims and the country as we go about the business of educating our students at Pace University.

Frank Monaco (cio@pace.edu) is the chief information officer at Pace University in New York.