Post-9/11 Emergency Response and Business Continuity Changes at Pace University and New York University

Donald Z. Spicer, ECAR
Bruce Metz, ECAR

ECAR Case Study 4, 2007
Post-9/11 Emergency Response and Business Continuity Changes at Pace University and New York University
EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology.

The mission of the EDUCAUSE Center for Applied Research is to foster better decision making by conducting and disseminating research and analysis about the role and implications of information technology in higher education. ECAR will systematically address many of the challenges brought more sharply into focus by information technologies.

Copyright 2007 EDUCAUSE. All rights reserved. This ECAR case study is proprietary and intended for use only by subscribers and those who have purchased this study. Reproduction, or distribution of ECAR case studies to those not formally affiliated with the subscribing organization, is strictly prohibited unless prior written permission is granted by EDUCAUSE. Requests for permission to reprint or distribute should be sent to ecar@educause.edu.
Post-9/11 Emergency Response and Business Continuity Changes at Pace University and New York University

Preface

The EDUCAUSE Center for Applied Research (ECAR) produces research to promote effective decisions regarding the selection, development, deployment, management, socialization, and use of information technologies in higher education. ECAR research includes

- research bulletins—short summary analyses of key information technology (IT) issues;
- research studies—in-depth applied research on complex and consequential technologies and practices;
- case studies—institution-specific reports designed to exemplify important themes, trends, and experiences in the management of IT investments and activities; and
- roadmaps—briefings designed to help senior executives quickly grasp the core of important technology issues.

From its most recent research, ECAR published *Shelter from the Storm: IT and Business Continuity in Higher Education* (Yanosky, 2007). The study provides subscribers with empirical information about where their business continuity vulnerabilities, plans, and practices stand in relation to surveyed institutions, and discusses factors associated with success in planning for the delivery of IT-dependent business services following a spectrum of potential service disruptions. Study results indicate that business continuity planning is commonly carried out among respondent institutions but that it is often incomplete and resource-constrained, and most plans are not tested.

Literature Review

Our review of the business continuity and disaster recovery literature focused particularly on the multiple standards that address these areas, including the ISO/IEC 17799 information security specification, the emergency-preparedness-oriented National Fire Prevention Association 1600 standard, and best practice frameworks such as the Information Technology Infrastructure Library (ITIL) and the Information Systems Audit and Control Association’s Control Objectives for Information and Related Technology (CobiT). In addition, we reviewed a wide range of secondary sources from disaster recovery and business continuity certification organizations and from the IT trade press, academic journals, and journalistic publications.

Online Survey

We e-mailed 1,615 EDUCAUSE member institutions, asking them to take our Web-based survey. Senior IT administrators at
340 institutions completed the survey. Most respondents held the position of chief information officer (CIO) or a comparable title indicating that they are their institutions’ senior IT leaders. The survey questions are on the ECAR Web site at <http://www.educause.edu/SurveyInstruments/1004>.

Interviews

We supplemented survey data with in-depth interviews with 15 IT and executive leaders from higher education institutions and corporations involved in business continuity efforts. In addition, ECAR designed the program for an EDUCAUSE business continuity summit sponsored by Microsoft at which 40 leaders from 36 universities and other organizations discussed business continuity issues in a facilitated-discussion setting.

Such interviews and forums enable us to deepen our understanding of the processes used for business continuity planning and testing as well as their results. They provide insight into the factors that drive business continuity planning and those that inhibit it. And they provide interesting examples of how institutions approach the many challenges inherent in this complex undertaking.

Case Studies

Researchers conducted this in-depth case study to complement the core study. We assume readers of this case study will also read the primary study, which provides a general context for the individual case study findings.

We undertook this case study to investigate how two institutions changed their thinking and practices after experiencing a major emergency. ECAR owes a debt of gratitude to Pace University leaders: Terrell Kolodzinski, executive director of General Services; Dennis MacDougall, vice president for Facilities Management; Frank McDonald, associate vice president for General Services; Frank Monaco, vice president for information technology and chief information officer; Frank Tramontano, director of IT integration and chief technology officer; Gerard Tarpey, director of computer systems; and Robert Yannocone, director of Network Services. Equally we wish to thank NYU leaders: David Ackerman, executive director, .edu Services and Digital Library Initiatives; John Beckman, vice president for public affairs; Henry Chung, assistant vice president for student health and director of the Student Health Center; Patricia DeLorenzo, senior director, Student Health Service; Ken Fauerbach, executive director, IT Planning, Compliance, and Continuity Services; Marie Gayle, executive director, Enterprise Computing and Support Services; Iris Harris, director of network administration and user support, Controller’s Division; James Kerr, director, emergency management and business continuity; Jules Martin, vice president, Department of Public Safety; Marilyn McMillan, associate provost and chief information technology officer; Efim Rubenchik, director, technical facilities preparedness; Charles Surendranath, assistant director for IT in the Department of Public Safety; Laura Tretner, executive director, Resource Planning and Management Services; and Alan Yood, associate vice president, operational risk management.

The authors wish to particularly thank their colleague, ECAR Fellow Judith Pirani, for her assistance in participating in one of the visits and in reviewing this study.

Rethinking Emergency Response, Disaster Recovery, and Business Continuity After 9/11

The ECAR study Shelter from the Storm: IT and Business Continuity in Higher Education (Yanosky, 2007) acknowledges that most business continuity plans at higher education institutions are not tested. This case study, however, takes an in-depth look at the actions two institutions, Pace University and NYU, undertook following their real-world testing in the 9/11 disaster. These institutions and
their response plans were tested again in the August 2003 Northeast regional blackout.

ECAR’s research study defines business continuity as an institution’s ability to maintain or restore its business and academic services when some circumstance threatens or disrupts normal operations. We understand business continuity to encompass disaster recovery, the activities that restore the institution to an acceptable condition after suffering a disaster, though business continuity also includes such matters as institutional risk assessment and prioritization of business processes. In this case study, as in the main study, we consider disaster recovery mainly in its traditional IT manifestation as maintaining IT operational capabilities in the event of an incident that compromises those capabilities. The institutions in this case study also added a response component in their planning—emergency response—which focuses on preserving lives and property during an emergency.

**Pace University Profile**

Pace University, currently celebrating its centennial, was founded in 1906 in lower Manhattan by midwestern brothers Homer and Charles Pace. Homer was an accountant and Charles an attorney, and they founded Pace Institute as a school devoted to preparing men and women in accountancy and business law to pass the New York State CPA examination. In 1947 Pace Institute became Pace College, a nonprofit, nonstock corporation. In 1973 Pace was awarded university status by the New York State Board of Regents. Currently, Pace University has multiple New York campuses. In New York City, there is a lower Manhattan campus as well as a midtown center. There are three Pace University campuses in Westchester County: one in White Plains, one in Pleasantville, and an administrative/residential campus nearby in Briarcliff. The location of these facilities was an important factor in Pace’s 9/11 response and subsequent emergency response, disaster recovery, and business continuity strategies. Until 9/11, there was an additional campus location, The World Trade Institute, in the North Tower of the World Trade Center.

In AY2006–2007, Pace had 8,928 undergraduate students, 4,471 graduate students, and 778 law students. Thirty-six percent of undergraduates lived in Pace University housing, and 64 percent commuted to Pace. Only 3 percent of graduate students were residential. Pace had 478 full-time and 760 part-time faculty.

In 2000, David Caputo became president of Pace University, shortly after a deadly dormitory fire at New Jersey’s Seton Hall University. While Caputo was not involved in the Seton Hall incident, it had a substantial impact on his view of universities’ responsibilities to prevent and respond to emergencies. He expressed this perspective early in his presidency by encouraging institutional sensitivity to the need for institutional plans for emergency response and disaster recovery. Although this theme had not yet been translated into operational plans by September 11, 2001, there had been preliminary discussions and studies.

The attacks on New York’s World Trade Center on September 11 had a direct impact on Pace and its community. The Pace facilities on the 55th floor of the World Trade Center Tower 1 were below the conflagration, and students and faculty who were in the building were able to evacuate. Tragically, four Pace University students and 60 alumni who were working for companies in the towers were killed. Their deaths had a significant impact on the collective psyche of Pace. Additionally, the Pace main campus is only four blocks from the World Trade Center. Together with the immediate area, it housed one thousand residential students. The Pace administration took advantage of the availability of multiple campuses to evacuate these students to Westchester County facilities during the period of emergency.
Several Pace administrators observed that while they had a weak plan prior to 9/11, they persevered due to the empowerment, initiative, and good sense of their on-site staff. For example, buildings and grounds staff members closed the fresh air dampers and shut down ventilation systems before the towers’ collapse and thus eliminated the risk of drawing contaminated air into their buildings. While these administrators also observed that no one can ever plan adequately for an event such as 9/11, soon after that event the university initiated a significant emergency response, disaster recovery, and business continuity planning process. The plan still will rely on the initiative and effectiveness of staff—and in fact makes that clear—but it also gives the staff processes, protocols, and training to support their ability to respond.

The Pace Emergency Response and Business Continuity Plan

As indicated above, thinking about the need for such a plan began in 2000 and was given substantial impetus by 9/11. According to Network Services Director Robert Yannocone, Pace had looked at disaster recovery plans for years but never had the resources to put one in place. Pace turned to their insurance advisors, Marsh, for advice regarding the structure of an effective plan to cover emergencies and business continuity in addition to traditional disaster recovery. Although they started in early 2002, it took until early 2004 to carry the plan development through to final approvals.

The plan is university-wide in scope but is intended for implementation at the campus level as necessary. As a further level of planning, each department is expected to develop a plan framed by a common Model Departmental Business Continuity Plan template, published in Section IV: Business Continuity Policy and Procedure of the university-wide Pace University Emergency Response and Business Continuity Plan (Pace University, 2006). The major components of this plan are:

- Crisis management policy and procedure, defining executive-level strategy development and implementation activities aimed at directing and managing all aspects of the response to and recovery from any emergency situation.
- Emergency response policy and procedure, specifying immediate actions aimed primarily at protecting people and property from injury or damage caused by any emergency situation.
- Business continuity policy and procedure, outlining activities, including substantial preplanning, aimed primarily at ensuring that all critical functions and operations continue to be performed during and after any emergency situation.

In the event of a major emergency, an executive-level crisis management team will be formed to manage the university’s total response and recovery effort. The team consists of the president and the executive council as well as representatives of the Offices of University Relations and Public Information, the executive director of safety and security, and the Office of Government and Community Relations.

The plan’s emergency response component operates at the campus level and is intended to guide emergency response personnel and resources during a major emergency. The senior member of the Pace security staff on duty will be the emergency response leader. This person will stabilize the situation, direct initial response, and notify the members of the crisis management team as necessary. Various departments will provide personnel and services as needed to form an emergency response support team. For example, the Division of Information Technology (DoIT) will maintain communication systems, Campus
Safety and Security will be the on-scene emergency responders, buildings and grounds personnel will manage damage control and buildings systems, Pace University Counseling Services will provide counseling as needed, and so forth.1

To support these groups’ needs, Pace has established five emergency communication centers around the university. This is one of the benefits of having multiple, widely dispersed campuses, although as will be seen, NYU has established three similar centers on its principal campus. These centers tend to be the size of an office or conference room, but they are well stocked with computers, printers, copiers, data and phone access lines, and emergency power. Normally, they are multiuse rooms that are maintained in a state of readiness for activation in the event of an emergency. In addition to connections to university communication services, the rooms are equipped to handle multiple cell-phone carriers, cable TV, and cable modems for redundant Internet access independent of the university connections. Additionally, each emergency communication center has up-to-date information including names, addresses, phone numbers, and emergency contacts for each of the various constituencies: students, faculty, staff, key suppliers, government contacts, and so forth, kept on CDs that are updated every three months.

Pace has emergency 800 number access on each of the three main campuses. The numbers are unpublished but can be publicized in an emergency. The university is prepared to establish call centers on demand. Additionally, accounts with Genesys Conferencing provide outside call center capabilities in an emergency or for severe weather response.

After 9/11, Pace replaced an externally supported Centrex system with an internal phone system designed with business continuity in mind. Each of nine PBX sites has its own voicemail system and an independent primary rate interface to the telecom central office. Each site is independent but is connected by voice over IP (VoIP) trunks over a Gigabit Ethernet backbone connecting the entire university. If the Gigabit Ethernet backbone is compromised in any location, service is not disrupted; instead, calls are then automatically routed “out of network.” Pace also has an old Nortel switch for the dormitories that can be put into service as a backup resource, if necessary.

**DoIT Disaster Recovery**

To support Pace’s emergency response and business continuity plans, DoIT must have traditional disaster recovery plans in place. “Prior to 9/11, DoIT had a disaster recovery plan in place,” according to Gerard Tarpey, director of computer systems for DoIT. “It was built with the idea that if something happened to the main data center we could take the necessary steps to recover and get mission-critical systems—SunGard Banner administrative applications, e-mail, and Blackboard Learning System—back up and running. However, I don’t believe that anyone in DoIT or Pace ever considered the type of emergency that appeared on 9/11.” He continues, “9/11 educated Pace to the realization that all disaster plans must be dynamic, forward-thinking, and ongoing.”

CIO Frank Monaco adds that “after 9/11, I no longer believe that any good IT disaster recovery plan will cover all possible contingencies. Now I believe that good disaster recovery plans should be flexible, practical, and rather general. The disaster recovery plan should point you in the right general direction. A maxim from the military fits: Violent execution, coupled with just the right amount of proper planning and guidance from the boss, are the real keys to success.”

After 9/11, Pace collected all central IT operations onto the Briarcliff campus. While this added efficiency to operations, it also introduced a single point of failure. Subsequent to 9/11, Pace established a near-real-time mirrored site in their downtown...
Manhattan campus. They take advantage of the Pace Gigabit Ethernet backbone. Chief Technology Officer Frank Tramontano observes that one lesson of 9/11 was the importance of having key services readily available without having to reconstruct them from tapes. However, even a gigabit connection is not sufficient to fully mirror all Pace systems in real time. Also, the cost of replicating everything is beyond the financial resources of higher education institutions.

As a result, as part of the Emergency Response Business Continuity Plan development process, Pace prioritized what it tries to replicate in backup. The priority items include the Oracle data supporting their Banner applications and the SQL component of the Blackboard application. As resources become available, DoIT hopes to replicate more applications. Each site has an independent, active network connection and Pace has a primary/secondary DNS server arrangement that allows the disaster recovery site to back up the primary DNS service. For Banner, Pace has four database instances of the system spread over four separate servers and one access server that fails over if one of the environments fails. Campus policy states that “sensitive data on desktop machines should be stored on a server,” and this server is backed up. Pace also offers Web storage for personal data.

All this being said, Tramontano observed that if he had it to do all over again, he would have spent more time investigating commercial alternatives. The model he would prefer would have Pace providing the hardware, applications, management, and support and the vendor providing the managed environment. “Uninterruptible power supplies, generators, and so forth are not core business for a university,” he said. As will be seen, NYU has taken the approach of letting a commercial supplier provide off-site disaster recovery services for mainframe-based applications and is using cross-campus mirroring for server-based applications.

Another change Pace instituted as part of the new disaster recovery philosophy is to design new systems with disaster recovery in mind. Tramontano emphasizes a modularized architecture so that modules can be transported to another environment in an emergency. Additionally, Pace seriously considers fault tolerance and scalability in every system implementation. Given the centralized nature of enterprise IT services at Pace, he can enforce these principles across the institution in his role as chief technology officer.

A final component of Pace’s IT disaster recovery strategy relates to staff. Key staff members have messaging services that provide access to voicemail either as voice messages or through e-mail, creating redundant communication channels that allow first responders to get detailed information whenever there is a problem. Systems are designed so that staff can log on from anywhere via a VPN connection for remediation.

**Business Continuity**

Business continuity inherently demands department-by-department activity. Pace has established a university-wide approach that ties affected departments together, ensures proper notification, provides necessary infrastructure, and gives guidance to local decision makers. As mentioned previously, each unit of the university is mandated to develop its own business continuity plan according to a model provided by the university. The university plan states:

The intent of the Departmental Business Continuity Plan is to minimize the amount of disruption any future emergency may cause to the department’s critical functions. This is accomplished by:

- establishing an administrative structure within the department to deal with future emergencies;
● investigating and preplanning appropriate responses to various types of potential emergencies;
● identifying and implementing changes to current operating procedures that will reduce the department’s susceptibility to disruption from certain types of emergencies;
● coordinating the department’s Business Continuity Plan with the plans of other departments that either provide services to or require services from the department;
● formalizing the department’s Business Continuity Plan in written form;
● maintaining a high level of knowledge and preparedness within the department of the department’s plans for continuing operations during emergencies (Pace University, 2006, p. 14).

Protocols developed to support this business continuity model plan deal with a wide variety of emergency events ranging from bomb threats, demonstrations and rallies, and various emotional distress and psychological emergencies to nuclear or hazardous materials contamination and catastrophic events.

The president and senior officers expect plan components to be viewed as living documents. The designated “keepers of the plan” are Frank McDonald, associate vice president for General Services, and Terrell Kolodzinski, executive director for General Services. As indicated above, the president came to Pace soon after a higher education disaster at another university, and Pace suffered one 18 months later. He is personally involved in dealing with every emergency event at the institution and is the chair of the crisis management team. However, effective business continuity requires broad, ongoing engagement by key members of the university community, and this requires effort to sustain, particularly because of normal personnel and student turnover. While those who had been at Pace during 9/11 have relatively strong memories of the event’s impact, that is not necessarily the case with new members of the community.

The institutional plan is regularly updated, and Pace offers training on its features several times a year. The campus security staff members are required to set up a communication center on each campus each semester (connecting all communication equipment). The president conducts periodic tests with no advance notice and asks members of the executive council (crisis management team) to report to the communication center on their respective campuses to test IT equipment and check staff and student rosters to see if they are up to date. Team members also review binders (Emergency Response Business Continuity Plan, division-wide occupancy, and building blueprints) to see if they are up to date. DoIT technicians test the IT equipment monthly.

Despite these energetic activities, Pace’s testing regime has some open issues. Individual departments must test their own plans. To date, other than fire drills, there have been no drills conducted that involve the overall community.

With respect to the plan’s future evolution, Pace is currently developing special protocols and plans for a possible avian flu pandemic. Such an international/national/regional health event is different in character from the events already in the plan. A planning committee is working on this under Frank McDonald’s leadership.

Pace officials agree broadly that any higher education institution could use the basic framework of Pace’s Emergency Response and Business Continuity Plan. That Pace has multiple campuses connected by a high-speed network certainly offers an advantage in implementing IT disaster recovery capability and distributing services, but this could be accomplished in other ways. As seen in the NYU case study that follows, combining coop-
erative interinstitutional arrangements and using commercial services could accomplish the same objective. Also, other institutional presidents might not want to be as personally involved, and presidential involvement has been a strong driver at Pace. The creation, implementation, and maintenance of a plan such as this do require a strong sponsor and strong general leadership support. Again, as demonstrated by NYU, support from the president and active leadership at the senior officer level may also be an effective model.

**New York University Profile**

In 1831 Albert Gallatin, who served as secretary of the treasury under President Thomas Jefferson, declared his intention to establish “in this immense and fast-growing city...a system of rational and practical education fitting for all and graciously open to all.” At that time, most students in American colleges and universities were members of the privileged classes. Albert Gallatin and the university’s founding fathers planned NYU as a center of higher learning that would be open to all, regardless of national origin, religious beliefs, or social background. Today, NYU comprises 14 schools and colleges at six major centers in Manhattan, the principal one being its Washington Square campus in Greenwich Village. NYU operates branch campus and research programs in other parts of the United States and abroad, as well as study abroad programs in more than 25 countries. NYU is also one of the largest employers in New York City, with more than 15,000 employees. In 2006, total enrollment was 50,917, of which 19,401 were undergraduates, 18,990 were classified as graduate or professional, and 12,526 were enrolled in noncredit programs.

**NYU and 9/11**

NYU’s size, diversity, decentralized organization, and the lower Manhattan location of the main campus present special challenges for dealing with emergencies, establishing emergency response, and planning for business continuity. The dense urban setting creates the potential for many events that could trigger emergency response activities. Some events occur within the university’s jurisdiction and community, while others occur in the neighborhood in which NYU operates. The tragedy of 9/11, for example, forced the evacuation and temporary closure of four residence halls just blocks from the World Trade Center. These housed approximately 4,000 students. At the main campus, approximately 1.5 miles from the World Trade Center site, classes were suspended.

At the time of 9/11, NYU had a plan for reacting to an emergency. It had a command center in place that could accommodate critical units necessary for a response, including Information Technology Services (ITS), NYU’s central IT unit. Immediately after the second tower of the World Trade Center was struck, NYU declared an emergency. Within 45 minutes of that declaration, the university’s emergency command center was fully operational.

The pre-9/11 plan and the command center were created by the NYU Department of Public Safety and used successfully to monitor the events and transition surrounding year 2000 (Y2K). The command center served as the key location where lines of communication were established with governmental agencies (federal, state, and local) to marshal the necessary resources to keep the university operational in the face of unique challenges. ITS also activated its command center to coordinate IT response to support university efforts such as developing a list of students displaced by the disaster and contacting them via e-mail (which most students received despite being displaced) to alert them to available services such as emergency cots at the sports center, laptop loaners, and hotel rooms. ITS immediately reconfigured its switchboard and help desk call centers to broaden the pool...
of people able to receive calls from worried parents and the public. The switchboard was kept open 24 hours a day for 10 days after the disaster.

NYU’s challenge was to care not only for those students displaced from their residence halls but also for the emotional welfare of the NYU community, including thousands of students who live on and off campus who were not displaced. Once the safety of the university community was determined, the question became when and in what way to reopen. With superb effort by the deans and faculty, NYU was able to schedule special programs and seminars on Friday, September 14, both to help the community deal with the trauma and to provide a place for students to go while normal operations were reestablished.

NYU Emergency Response and Business Continuity Planning Since 9/11

In the aftermath of the 9/11 tragedy and the Northeast blackout of 2003, NYU has engaged in serious reevaluation of its institutional emergency response and business continuity plans and processes. While the 9/11 response in particular was as good as could be expected under the circumstances, NYU wanted to learn from these events and make emergency response and business continuity improvements in preparation for responding to future incidents.

“Our response to 9/11 was the work of very dedicated people to an extreme emergency,” notes Ken Fauerbach, NYU’s executive director of IT Planning, Compliance, and Continuity Services. “NYU was indeed able to take advantage of its emergency planning at that time, but it recognized that to effectively respond to the breadth of emergency represented by 9/11 and the blackout of 2003, it needed to develop a more robust and far-reaching emergency plan.” An emergency response plan was developed with the assistance of James Lee Witt Associates in 2005 and 2006. NYU is now evaluating how to break down this plan into small operational components to better serve the university.

Since 9/11, NYU has instituted a robust notification plan called Emergency Notification and Communication Systems (ENACS). The new plan designates several tiers of response and responders. It creates an incident response team composed of five members of the university leadership team representing both academic and administrative sides, and an incident response and command structure led by the director of emergency management and business continuity and the vice president of public safety. The plan also designates 15 functional units including ITS that are essential to ensuring the operation of the physical and electronic infrastructure, along with providing key human resource support and financial functions.

When an emergency occurs, generally a senior member of Public Safety responds to the scene. This individual determines the nature and scope of the problem and initiates communication via ENACS with the incident response team. If warranted by the emergency, alerts can also be sent via recorded message to representatives of various organizational groups, such as the 15 operations departments or the full university leadership team. The incident response team determines whether an emergency should be declared and who among senior university leadership should be notified, if they are not already involved.

To eliminate a single point of failure, NYU now has three geographically diverse, strategically located command centers. The team decides whether to activate a command center, now called the Emergency Operations Center, and which of the three possible sites would be most appropriate. Throughout the crisis, audioconferencing, as well as e-mail and text messaging, can be used to commu-
nicate between and among the incident response team members and key constituencies. Communication with the university community and the public is coordinated by Public Affairs in conjunction with the incident response team. NYU has a predesignated Web site and university hotline telephone number, connected to a mass announcement system, to provide information and status. The philosophy is that it is important to respond promptly to the situation, gather critical data, and present the information to the senior university leadership to assist in their role as the initial critical decision makers. NYU has invested in mass communication software to enable group calling and is reevaluating both the software being used and how to make the most effective use of this capability.

Much of NYU’s view toward emergency response and business continuity can be discerned from staffing decisions made in recent years. Alan Yood, who was senior director of Environmental Services and was charged with creating an emergency response plan subsequent to 9/11, has recently been appointed associate vice president for operational risk management. In this role, he will look at institutional risk factors, their potential impact, and mediation. The scope of activity covers all facets of operating a major university and ranges from NYU’s New York campuses to its international programs. This office will have five analysts on staff; however, the intent is to reach out to the academic schools and functional offices.

Yood observed that after 9/11 there was a dramatic change in thinking about emergency response and business continuity at NYU. In particular, he said, “Prior to 9/11, emergency response/business continuity were considered, but in a singularity perspective—such as loss of a building due to fire. Post-9/11 [there was a] realization that emergency response/business continuity had potential to address multiple issues in a one-incident construct. That realigned management thinking that a formalized structure was needed to address the possibilities.” There was a refinement in communications processes and formalization of protocols for dealing with the issues surrounding an emergency and mitigation of its effects. High on the agenda in the near term is planning for a possible avian flu pandemic, in which James Kerr, director of emergency management and business continuity, has taken the lead in developing the university’s plan. Kerr reports to Jules Martin, vice president, Department of Public Safety. Yood and Martin both report to the senior vice president and general counsel.

Kerr’s hiring in late 2005 from Consolidated Edison Company of New York (Con Edison), a utility and energy company, is another staff appointment of significance to this study. His role is to bring all of NYU’s business continuity components together. The creation of such a position is currently atypical in higher education institutions but may suggest a trend as higher education grapples with the growing prevalence of security and emergency events. Kerr feels that urban institutions in particular need to look at creating such a position. In his opinion, coming from outside the higher education community and being well connected to the external mutual aid community is a plus for someone required to be an agent of change. Connection with key vendors and governmental agencies is also a critical attribute. NYU now has a seat in the New York City Emergency Operations Center as representative of 15 independent higher education institutions in the region. NYU also found that depending on traditional media is no longer adequate for timely decision making. During the 9/11 event, media increasingly focused on the human interest aspects of the incident and did not provide enough specific details for those who needed to respond to events on behalf of their organization. Additionally, the ability to have person-to-person contact
with key city governmental personnel is vital. Kerr is liaison to local fire, police, and emergency management agencies at various levels.

Kerr notes that the ability to communicate in all dimensions is the most important issue in an emergency. By this he means both horizontal and vertical communications with his peers in emergency management outside NYU and with senior officers, deans, faculty, staff, and students within NYU. Recognizing the importance of all types of communications in an emergency, NYU currently has a committee looking at communication strategies both within and outside the university, with the goal of standardizing and integrating equipment purchased by the university’s many departments.

IT organizations have always given disaster recovery a high priority out of a sense of self-preservation and more recently because it is a component of regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and a concern of auditors. Disaster recovery is generally perceived as a matter of operational continuity. In addition to institutional events, IT has to be concerned about fires, floods, hardware and software failures, electrical outages, security breaches, and human error in planning for failures in operations. From this perspective, ITS at NYU has historically invested in disaster recovery activities in a manner appropriate for a major research university. But since 9/11, Marilyn McMillan, associate provost and chief information technology officer, has emphasized the need to look outside the specific needs of ITS and build bridges to the university as a whole relating to business continuity. McMillan emphasizes that “Today, IT is an essential ingredient in so many aspects of the university’s capacity to handle disasters. IT professionals have moved out of the back room into full partnership with their colleagues throughout the university in planning for and responding to emergencies. At NYU, our innovations to make this transition and step up to these new expectations and responsibilities, while we keep everything else running, also have strengthened other areas of our work.”

In addition to charging Ken Fauerbach with coordinating its emergency preparedness planning, ITS created a position of director, technical facilities preparedness. Held by Efim Rubenchik, this position is charged with reaching out to the university’s distributed business and academic units to assist them in developing and implementing continuity of IT operations plans that articulate with those of ITS. In this activity, he partners with James Kerr. The need for Rubenchik’s position is driven in part by the distributed nature of operations at NYU: Many units run local IT operations to support their activities. More significantly, it is driven by ITS’s experience and professional skill set, often not available among local IT administrators. Rubenchik observed that designing, testing, and implementing disaster recovery and business continuity plans is a full-time job and cannot be done properly as a part-time activity by someone with significant day-to-day operational responsibilities.

Certainly, 9/11 was also a wake-up call to these offices, but there have been subsequent events, such as a blackout in 2003 and a heat emergency in the summer of 2006. The latter required shedding power from “low priority” electrical systems in the New York City area. These events have driven home the fact that “emergencies happen.” Rubenchik’s services are delivered on a fee-for-service basis to individual schools or departments. This funding approach reflects ITS’s desire to develop an outreach service within the dominant “every tub on its own bottom” funding model in operation at NYU. ITS has expertise but is not funded to provide it to every unit at the institution, and if it were, demand would likely outstrip capability. The approach taken is much more sustainable and scalable. Units
using the outreach service pay a share of its cost. ITS is taking the lead and the risk in developing the service initially.

Rubenchik’s first “customers” have been the Controller’s Division and the Student Health Center. (He is also in discussion with the Stern School of Business.) Why these offices have turned to Rubenchik and ITS is instructive. Both units are housed in rented space in the same building off campus. During 9/11 and the 2003 blackout, the landlord closed access to the building, although the Controller’s Division had to get a payroll out. Eventually, the staff was able to gain access to the building and handle the payroll, but the Controller’s Division realized that they needed a better plan.

The Student Health Center, on the other hand, was considered a critical service during the 9/11 closure of the area, and their personnel were allowed into the building. Their need today for continuity of operations support relates in part to HIPAA’s information security requirements. The center had made several unsuccessful runs at developing a disaster recovery/business continuity plan, and its leadership decided that they needed professional help. The solution was to move their servers to the ITS Data Center, which provides security, systems management, and disaster recovery services. The Controller’s Division had temporarily taken the same path, but when their application vendor offered off-site hot-site services, they moved to that solution. In their case, disaster recovery is a complicated three-legged stool. A separate company collects and stores backup tapes, and in the event of an incident, the tapes must be moved to the application vendor’s hot site. Both the Controller’s Division and the Student Health Center feel they have addressed the physical aspects of a business continuity plan, but they also agree that business continuity is an ongoing issue. They are now turning their attention to the “people issues” related to business continuity.

**ITS Disaster Recovery and Business Continuity Plans**

While ITS had a disaster recovery plan prior to 9/11, it has invested substantially in improving it based on the lessons learned from that event as well as from the 2003 regional blackout. Fauerbach observed specifically, “The blackout of 2003 helped us to see the vulnerabilities in the power supply to key systems, even those with extensive battery backup. As a result, the university invested in extending electrical feeds from its cogeneration plant to several key machine room sites. Now several key sites have dual power supplies [utility feed and cogen feed].” Additionally, ITS has created an on-call system of “flight directors,” that is, ITS directors who are scheduled to be on call to take charge in the event of a serious incident or emergency. Each director has a specified week as flight director and a week as backup on a roughly two-month rotation. Currently there are 11 designated staff in this rotation, each supplied with an extensive *Flight Director’s Handbook* giving detailed information and instructions on how to activate the primary ITS Command Center and/or its backup command center and support communications both within ITS and with the university community at large.

The handbook also has a database of facilities, contacts, and procedures. Each command center, as well as ITS office areas and machine rooms, is stocked with water, nonperishable food, flashlights, light sticks, and other emergency gear. Additionally, all ITS staff members have detailed instructions on shelter-in-place, building evacuation and assembly location instructions, and knowledge of a designated alternate site to go to if an emergency affects their facility.

Off-site arrangements also have been created. NYU has partnered with the University of California at Berkeley, MIT, and NYU in Florence, Italy, for backup DNS and Web hosting services. In terms of disaster recovery for application service, NYU has contracted...
with SunGard for warm-site services. NYU has had a disaster recovery subscription for almost 20 years, focused initially on mainframe applications. While it still maintains its student and human resource information system applications on a mainframe, it has expanded its subscription to include other principally administrative applications such as its financial and development systems, and also to cover its extensive server farm environment. After NYU officially declares an emergency, SunGard will acquire off-site stored backup tapes and NYU staff will go to a remote operations site. Within 48 hours, NYU-supported services should be recovered. Annual disaster recovery testing has proven that full system, application, and network recovery can be accomplished in just over 24 hours once staff have arrived on site. After 90 days on emergency status, NYU will be responsible for providing equipment at a SunGard-supported location.

NYU employs on-site, mirrored systems for its portal, Web server, e-mail, and learning management systems. These systems are distributed servers across multiple buildings and share a dedicated network. For the longer term, the state network, NYSERNet, is considering developing a remote disaster recovery site for connected organizations. NYU is in discussion with them regarding participation.

Rubenchik and his colleagues have developed tabletop exercises to test the plans, and the ITS team engages in a full test scenario of the SunGard service annually. Fauerbach observed that preparing for and conducting a disaster recovery test is a priority for ITS in its list of activities. David Ackerman, executive director, .edu Services and Digital Library Initiatives, said, “Working on emergency response and disaster recovery planning and testing has made life much less stressful. Everyone knows what to do when an event actually occurs. It has lowered the stress level of the organization.” Also he observed, “Having been through what we have been through, we feel tremendously prepared.”

Marie Gayle, executive director, Enterprise Computing and Support Services, added, “One of the things that ITS has learned to do well is coordination, knowing, for example, who needs to stay at work initially and who needs to be sent home to return as rested replacements or to work from home. People tend to stay calmer in an emergency when they have been trained.” Marilyn McMillan emphasized that emergency response and disaster recovery plans need to take the people aspect into account and not just plan for things and services. Fauerbach quoted something he learned long ago: “In an emergency you have crisis and chaos. You have to eliminate the chaos and deal with the crisis. Planning and practice tend to reduce the chaos.”

Some Comparisons and Contrasts

While both Pace and NYU are New York City-area institutions, and both were affected by 9/11 and the 2003 Northeast blackout, their approach to business continuity reflects their individual organizational dynamics. NYU is highly decentralized with a strong tradition of local autonomy at the school level. Pace is much more centralized in terms of decision making, services, and planning. Mirroring this dynamic, Pace developed an institution-wide emergency response, business continuity, and disaster recovery plan with a template for individual units. NYU created an institution-wide emergency response plan but currently depends on much more local autonomy in developing and implementing business continuity plans.

The role of central IT in supporting emergency response and business continuity has some commonalities across the institutions and some differences that reflect the institutional culture. In both cases, the central IT organization developed effective, but different, approaches to ensure traditional
IT disaster recovery. Equally, each developed and implemented communications capabilities for the institution as a whole in the event of an emergency. Since most enterprise applications are centrally supported at Pace, the DoIT disaster recovery capabilities automatically translate into core disaster recovery for all of Pace’s departmental business continuity needs. At NYU, that is not always the case, so additionally ITS is offering either disaster recovery–supported machine room space or disaster recovery consulting services to the academic and business units of the university that have locally supported critical applications. ITS is also coordinating with university emergency management to extend awareness of the university’s IT business continuity environment. NYU’s business continuity, disaster recovery, and emergency response environment is a reflection not only of the increase in staff with an express focus in those areas but also of the related projects initiated at the university. Fauerbach observed that “NYU is serious of purpose in highlighting and raising the quality and importance of the conversation university-wide concerning business continuity, disaster recovery, and emergency response and in emphasizing its commitment to continuous improvement in those areas.”

**Lessons Learned**

The experiences of Pace and NYU provide some valuable lessons that institutions can learn from to deal effectively with the increasingly difficult, complex, and important areas of business continuity, disaster recovery, and emergency response.

- **The quality and resourcefulness of people are key.**

  In an emergency, successful response comes down to the ability of the people involved to rise to the occasion. Indeed, while much of traditional IT disaster recovery has focused on hardware, software, and data, recent disasters, such as 9/11 and Hurricane Katrina, have shown that people are the most important part of the response effort. Both Pace and NYU emphasized that while their plans were incomplete at the time of 9/11, they persevered through the emergency due to the experience and capabilities of the people on the ground. It was also observed at each institution that a baseball analogy applies: Some teams invest in high-priced players but don’t have a real team approach; others invest in building a team. In an emergency you need the second model to be in place.

- **Start planning regardless of resources.**

  Recent incidents demonstrate that in addition to making sure the necessary people are involved, having at least some semblance of a plan is critical. Without proper business continuity/disaster recovery planning, respondents may not know what to do, where to go, or how to communicate. For business continuity, plans become the framework for maintaining essential capabilities and ensuring that the people dealing with a disaster or business disruption are working toward a common end as effectively as possible.

  Given the potential scope of emergency response, disaster recovery, and business continuity, waiting for an assurance of the resources necessary to undertake comprehensive initiatives in these areas means nothing will likely be done. In fact, many planning components are organizational and require a change in thinking and process but probably relatively few resources. For example, this study reveals that basic parts of an effective plan include

- structuring response teams,
- defining roles and responsibilities for the teams,
- establishing lines of communication,
- identifying the chain of command and decision-making authorities,
- allowing for flexibility should the unanticipated occur during a disruption or expected recoveries fail, and
providing for regular plan review, testing, and updating.

We should note that many with whom we talked in this case study observed that while the framework plan may need to be holistic, its implementation can be broken down into a series of activities to be put in place as resources become available. Moreover, study participants regularly commented that no disaster recovery/business continuity plan can cover every possible contingency. There are always aspects of a plan that require decision making in the context of a disruption or emergency, no matter how thorough the planning process. Ensuring that the plan basics are covered can help offset disaster recovery/business continuity resource limitations.

Disaster recovery/business continuity planning benefits daily operations.

Efim Rubenchik observed that “Every issue related to disaster recovery/business continuity has led to improvement in normal operations.” Generally these planning activities are viewed as buying insurance in the event of an emergency. Typically, however, thinking through the issues related to incident response involves analyzing normal operations. Specifically, Fauerbach noted, “Compliance with regulations, such as HIPAA, security, or the work associated with planning for a disaster recovery test, is often regarded as a tail that wags the dog, but such activities often expose gaps in documentation, deficiencies in training, and vulnerabilities in the operational environment. For example, [ITS] now has more individuals cross-trained on systems, more in-depth systems documentation, including extensive recovery scripts, and we have improved our daily backup procedures.”

As the experiences of Pace and NYU have shown, results of this exercise can lead to better decisions about IT overall, which in turn are likely to produce performance, reliability, security, and related gains in the regular delivery of IT services.

Professional assistance can be valuable in developing and implementing disaster recovery/business continuity plans.

This case, along with other ECAR studies, shows that business continuity planning has grown more sophisticated over the past several years, going well beyond the technical recovery of IT systems and services. Clearly, at this stage emergency response and business continuity are not necessarily core internal capabilities for higher education institutions. As a result, both Pace and NYU decided that to develop appropriate plans in a timely fashion they needed to get outside professional assistance. Disaster recovery and business continuity issues have such significant enterprise impact that an investment in external resources will likely have an attractive cost-benefit ratio while also providing needed expertise or capabilities not readily available within the institution.

Institutional leadership matters.

As in past ECAR studies of other enterprise-wide issues, the success of disaster recovery/business continuity initiatives is highly dependent on strong support and involvement by institutional leadership. Both Pace and NYU have the necessary level of commitment from the president and key vice presidents. The NYU experience shows that the leadership of a key unit, such as ITS, can provide a model and services that help other units implement business continuity. At the same time, to achieve broad effect and to do so in a timely fashion, active involvement from the top is required. This involvement goes a long way toward communicating the vital importance of disaster recovery/business continuity preparedness to all members of the institution, helping ensure that people take their part in the process with an appropriate level of seriousness and dedication.

IT can take a lead role.

For initiatives such as emergency response and business continuity, almost every unit depends on IT services, and, as previously
mentioned, a key element of any emergency response plan is communication. Success thus depends on significant involvement by the IT organization. Also, IT units have considerable experience in developing, implementing, and testing disaster recovery capabilities. ITS built on this experience to offer a consulting service to other departments to help ensure that different areas of the institution are engaged in the disaster recovery/business continuity process. IT organizations might consider this model in assisting their institution to effect emergency response and business continuity plans.

When implementing such a consulting model, IT organizations should focus on leveraging their disaster recovery expertise while stopping short of taking ownership of the business continuity process. Fundamentally, business and local units must manage their business continuity and disaster recovery efforts and be accountable for them. Therefore, these activities are best owned by the relevant academic and administrative departments as well as by the institution’s senior leadership.

- **Build disaster recovery/business continuity and security into every project and IT service.**

A common theme of recent ECAR studies of IT security reiterated here is that disaster recovery, business continuity, and security need to be designed into projects from conception through implementation. Given their degree of criticality and complexity, issues of business continuity and operations security can no longer be added effectively after the fact.

As a result, IT services need to be designed with business continuity in mind. Pace’s Tramontano observed that “after 9/11, whenever Pace designs a service or implements a system, they do so in a modular manner and give consideration to how it easily could be transported to a new environment.” ITS at NYU includes disaster recovery/business continuity as part of its project planning process to build it in from the outset. The message is clear: If one does not consider early on the possibility of reestablishing a service in a new location subsequent to an incident, it may be very difficult and expensive to do so when the need arises.

**Transportability to Other Institutions**

The Pace emergency response and business continuity framework is based on a multilevel planning model consisting of enterprise plans to deal with institution-wide issues complemented by department plans to deal with locally based issues. While the implementation details are specific to Pace, the framework that outlines the elements of what should be done by whom and when is very applicable to other institutions. Additionally, this plan provides a template to help individual departments, both academic and administrative, develop their local plans. This template, along with the associated common planning requirements and protocols, should be transportable to departments elsewhere. Ultimately, the applicability of a multilevel planning approach for a particular institution will depend on the institution’s degree of organizational complexity and extent of decentralization.

A key component of incident response is communication. Both Pace and NYU developed a variety of redundant communications vehicles for all constituencies—first responders, officers, middle managers, community response organizations, and the broad university community. While variations may depend on institutional organization or the local physical context, the issues they have dealt with and the solutions they have come up with would be informative to organizations everywhere.

NYU has invested in staff whose charge is to coordinate emergency response and business continuity plans and activities across the
institution. These staff felt that the investment was atypical at this time but that institutions increasingly recognize the need to provide dedicated staff to establish a framework for incident response and operations continuity and to maintain momentum for these activities. A university has many interdependent “moving parts,” and to ensure that all critical parts have emergency response and operations continuity plans that are continually maintained, tested, and ready to be put into effect is an activity that cannot be done well on a part-time basis.

Conclusion

As illustrated in the ECAR research study on business continuity, Shelter from the Storm: IT and Business Continuity in Higher Education (Yanosky, 2007), business continuity has moved higher on institutions’ list of priorities. Because of the broad impact of recent incidents, disasters can no longer be seen as something that happens to someone else. Potential disasters may affect whole regions or the entire country, and university administrations and boards are deciding that their institution may well be at risk. This case study has examined two institutions that have experienced several serious incidents. While neither feels it is completely prepared for the next event, each feels that it has made substantial progress. More important, they view this as an ongoing activity in which they continue to invest resources. Several of those with whom we spoke said that no one can fully prepare for an event such as 9/11, but they, their staff, and their university community will be much better prepared to respond if a comparable event occurs in the future.

Endnotes

1. Appendix C of the Pace University Emergency Response and Business Continuity Plan gives a detailed checklist of duties and responsibilities of the crisis management team members.

2. The breakdown of offices NYU included in the Emergency Notification and Communications System call list may have value for other institutions. Initial notifications are sent to the initial response team (VP for public safety, VP for public affairs, senior VP and general counsel, and senior vice provost for undergraduate education and university life) and then key representatives from Animal Facilities, Central Plant, Dental Center, Facilities Management, Human Resources, Medical Center, Public Safety, Student Health Center, Information Technology Services, Campus Planning and Real Estate, Construction Management, Environmental Health and Safety, Legal Counsel, Public Affairs, Student Affairs, Student Housing, and Emergency Management.

References

