Seizing the Moment:
A New Model for
Disaster Recovery at
Florida State University

Judith A. Pirani, ECAR
Donald Z. Spicer, ECAR

ECAR Case Study 1, 2007

Case Study from the
EDUCAUSE Center for Applied Research
Seizing the Moment: A New Model for Disaster Recovery at Florida State 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.
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—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 higher education with empirical information about where its 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 in higher education but that it is often incomplete and resource-constrained, and most plans are not tested.

Literature Review

ECAR’s 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 of the International Organization for Standardization and the International Electrotechnical Commission, the emergency-preparedness-oriented National Fire Prevention Association 1600 standard, and best practice frameworks such as the IT Infrastructure Library (ITIL) and Control Objectives for Information and Related Technology (CoBIT). In addition, we reviewed a wide range of secondary sources from 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.

**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 participated in a two-day business continuity summit sponsored by Microsoft and hosted by EDUCAUSE, at which 40 attendees representing 36 institutions 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, along with 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 examine how Florida State University (FSU) uses high-speed networking to deliver disaster recovery and business continuity services from a remote site. ECAR gratefully acknowledges the support of the following individuals in the preparation of this case study: Lawrence Abele, provost and executive vice president of academic affairs; William Agner Jr., ERP analyst II; Carl Baker, program director, Office of Technology Integration; Michael Barker, director, University Computing Services; Michael Barrett, assistant vice president, Office of Technology Integration; Jeffrey Bauer, assistant vice president and chief technology officer; Rick Burnette, associate director, Office of Admissions; Larry Conrad, associate vice president for technology integration and chief information officer; Mikal Haney, technology specialist, Northwest Regional Data Center; Kenneth Hays, network specialist, Office of Telecommunications Networking; Diana Key, assistant director, Sponsored Research Services; Ethan Kromhout, assistant director, University Computing Services; Joseph Lazor, director, Information Resource and Security Management; Angela McCausland, director, Enterprise Resource Planning; Randy McCausland, director, Information Services Infrastructure; Beverly Miller, assistant director, controller’s office; Thomas Morgan III, technology specialist, Office of Technology Integration; Mary Stephenson, assistant director, University Computing Services; and John Winston Jr., business analyst, Office of Technology Integration.

**Introduction**

Disaster recovery and business continuity address a fundamental IT premise: “If you have a man-made or natural disaster or hacking incident, and you don’t have a place to access and restore uncorrupted data in a meaningful way, you’re cooked,” states Joseph Lazor, FSU’s director for Information Resource and Security Management.

A near miss by Hurricane Katrina in late August 2005 forced the FSU Office of Technology Integration (OTI) to address this premise head-on. In recent years, OTI has started to host server-based enterprise resource planning (ERP) and course management system (CMS) implementations. As a result, their mainframe disaster recovery strategies needed to be reevaluated. “We invested all this money into our ERP and CMS with local fault tolerance and redundancy, but when Hurricane Katrina was threatening...”
the Tallahassee area, we realized we had to also address remote business continuity and disaster recovery,” states Carl Baker, OTI program director.

Hurricane Katrina veered off, sparing FSU but leaving an indelible impact on Larry Conrad, FSU’s associate vice president for technology integration and chief information officer. Unwilling to repeat the experience, Conrad vowed to create a remote disaster recovery/business continuity site for FSU’s server-based systems by the start of the 2006 hurricane season. Although pressed for time and money, OTI successfully implemented a remote site in Atlanta in early June 2006 by leveraging available resources and technologies, including:

- a recently completed FSU business impact analysis to foster business user and senior administration buy-in, to create a financial business case for the project, and to identify the core set of business functions to be supported by the remote site;
- senior administration support, especially from the provost and executive vice president of academic affairs, for IT in general and for the remote disaster recovery/business continuity site project in specific;
- Florida LambdaRail (FLR), National LambdaRail (NLR), and the regional Southern Crossroads GigaPOP networks to provide a high-speed and cost-effective networking conduit for backing up data to the remote site; and
- virtualization technology to reduce the Atlanta site’s footprint requirements and facilitate remote system administration.

“It is easy to get lulled into a false sense of security,” states Lawrence Abele, provost and executive vice president of academic affairs. “Many FSU buildings are built to withstand up to 200-mile-per-hour winds; we have many backup systems; but you can never do too much, as the cost to us to deal with the aftermath of losing critical data would be considerable.”

This case study details how FSU turned its wake-up call into an opportunity to implement its remote IT disaster recovery operations site. It begins with a background overview of FSU; proceeds to examine environmental alternatives and implementation; looks at challenges, benefits, and lessons learned; and concludes with a discussion of this solution’s transferability to other institutions.

**Institutional Background**

In 1856, Francis Eppes, intendant (mayor) of Tallahassee, generously donated a boys’ school land and buildings to the state legislature, providing the genesis for Florida State University. Today, FSU’s 16 schools and colleges offer more than 300 undergraduate, graduate, doctoral, professional, and specialist degree programs, including medicine and law, to its approximately 40,000 students. FSU generated more than $160 million in external grant support in the fiscal year ending June 2005.

At FSU, disaster recovery falls under the domain of the Department of Environmental Health and Safety, which reports to the Division of Finance and Administration. FSU’s Emergency Management Plan OP-G-1.9 <http://www.safety.fsu.edu/emermanplan.html> defines lines of authority, describes the Emergency Planning Committee and Emergency Operations Center, outlines responsibilities and communication notification, and establishes procedures for managing employee leave and payroll. Currently, disaster recovery and business continuity make up part of the director of environmental health and safety’s management portfolio, but the university has identified an institution-level emergency manager position to focus more extensively on this area.
Office of Technology Integration

During late spring and summer of 1999, FSU reorganized its IT operations under a new vice president and formed OTI. Larry Conrad is responsible for academic computing, administrative computing, and telecommunications for the university. OTI includes several departments:

- Information Resource Management provides technology resources management, support, and security services for OTI and the campus as a whole.
- Information Services supports the enterprise business processes. This includes FSU’s Online Management of Networked Information (OMNI) PeopleSoft-based ERP system plus its Blackboard-based CMS system. Conrad notes that FSU is “a large Blackboard site. The vast majority of FSU courses use at least one component of Blackboard to augment the classroom situation.”
- The Office of Telecommunications manages FSU’s voice, video, and data networks as well as campus access and security systems and call center services.
- University Computing Services manages the university’s central computing facility and works in conjunction with FSU colleges and departments to provide services to help meet university computing and networking goals.
- User Services provides IT support for FSU’s students, faculty, and staff.

Additionally, the Northwest Regional Data Center (NWRDC), while not a component of OTI, works very closely with OTI in several relevant areas. The NWRDC is an independently funded auxiliary of FSU that provides systems support and applications, IBM’s z/OS, Web services, and mainframe-based hosting services as well as disaster recovery, data storage, vaulting, and backup storage services to both educational and governmental entities. The organization owns a 14.3-mile fiber-optic ring around the Tallahassee metropolitan area. Though a separate entity, the NWRDC is hosted by FSU and located on the FSU campus, near the University Computing Services facility.

As with many large research institutions, the FSU IT environment is decentralized. For example, FSU maintains three separate e-mail environments for students, faculty, and staff. Some departments have chosen to maintain and staff local IT operations. However, University Computing Services does offer colocation space in its computer facility for FSU departments, and OTI has observed a swing back to centralized systems management, spurred in part by IT security requirements and staff turnover.

When the state of Florida changed FSU’s status in the School Code Rewrite in 2001, it impacted FSU’s enterprise systems as well. Before this legislation, all Florida state universities were governed by a board of regents and were considered to be state agencies with the right to use the state of Florida’s accounting and payroll systems. At this point, the preponderance of FSU data was mainframe-driven and -stored; the board of regents had established regional data centers where all critical data resided. The education code rewrite, however, abolished the board of regents. In turn, it established a board of trustees for each state university, designated each as a public corporation, and removed each institution’s state agency status. Consequently, FSU and other state universities could no longer use the state’s financial systems, forcing them to transition to their own financial and payroll systems.

FSU decided to take a two-pronged approach to enterprise systems. The university evaluated ERP systems with other Florida institutions, eventually purchasing a PeopleSoft ERP system jointly with the University of Florida and Florida Agricultural and Mechanical University. Ultimately, FSU implemented the OMNI service during 2004–2005, which consists of
PeopleSoft financial, human resources, and payroll systems. Most student information is still maintained on a legacy, mainframe-based student information system, which is hosted by the NWRDC. “Student information is a mixture of the mainframe and open system architecture,” states Randy McCausland, director of Information Services Infrastructure. “It is fairly complex in that no single solution can address the entire student information area. The NWRDC can handle 80 percent of the need; 20 percent is handled through other ways.” OTI provides Web-based middleware to create a portal-like access environment to OMNI. The new PeopleSoft system is located at the NWRDC facility, with responsibility and support falling to the University Computing Services UNIX group.

**Dual Environment Leads to Separate Approaches**

FSU’s transition to an ERP environment posed new business continuity and disaster recovery issues as well. FSU is statutorily mandated to have a disaster recovery plan for the entity where its critical data resides. “In the past, we always relied on the NWRDC to have viable business continuity and disaster recovery plans,” states Joseph Lazor. “We came to the realization when the ERP system came into the mix that it was going to be a different and more complex type of environment above and beyond the mainframe. We began to see a greater need to have a two-pronged approach.” This was especially true since the Web-based access to the mainframe-hosted student information system meant that both the FSU ERP and the mainframe systems must be up and running to complete some business processes.

**Traditional Mainframe Environment Uses Straightforward Method**

The NWRDC relies on traditional disaster recovery for its operations. Though the NWRDC is situated in a building designed to withstand 150-mile-per-hour winds, it conducted a request for proposal process in 2004 to select a hot site at which to restore its business services. In 2005 it eventually chose IBM to provide disaster recovery services at the company’s Sterling Forest, New York, site. NWRDC personnel must transport data tapes to restore the center’s operations at the IBM site.

**Twists and Turns Lead to an Innovative Approach for Server-Based Systems**

The implementation was less straightforward for OTI’s server-based information systems. Hurricane Katrina did reveal the need for a remote backup site, but the project’s roots can be traced back to a business impact analysis (BIA) that was literally wrapping up as the storm tracked up the coast of Florida. The BIA results offered guidance as OTI moved forward with the remote backup site project in fall 2005.

**BIA Identifies Priorities, Triggers Awareness, and Lays Fiscal Groundwork**

As part of the NWRDC mainframe disaster recovery planning in 2005, IBM offered a BIA to all NWRDC clients to identify both the financial and intangible losses that might be sustained during an extended business disruption; to identify the critical business processes that most affect FSU’s revenue and operations during this period; and to prioritize recovery strategies. The process provided estimated tangible and intangible losses, recovery time objectives for restoring process operations, and data recovery-point objectives to rank the recovery order of FSU’s critical business processes. Coincidentally, the new ERP system had just gone live. Recognizing that ERP-related business continuity/disaster recovery planning needed to be addressed, OTI and ERP management jointly requested that ERP
business processes be added to the scope of the BIA project. Numerous FSU administrative areas participated in the project, including

- Office of Admissions and Records,
- Office of Withdrawal Services,
- Orientation Center,
- University Housing,
- Office for Distributed and Distance Learning,
- Payroll Services,
- Purchasing & Receiving,
- Office of the Controller,
- Office of Sponsored Research Services,
- Office of Human Resources,
- Office of Financial Aid,
- Athletics Department Administration,
- Office of Undergraduate Studies,
- Division of Student Affairs, and
- the International Student and Scholar Center.

During the summer of 2005, FSU facilitated a combination of small-group and one-on-one internal meetings with the business managers involved with financial, human resources, payroll, and student information business processes. Using an IBM-provided software tool, the meetings derived information about each area’s critical data, the maximum process downtime the area could experience with minimal impact, and the “oldest” data state that each area could use to restore operations. “Our strategy was to employ the functional directors of the ERP project to coordinate the work sessions with their own office staff to provide the actual input,” states Thomas Morgan III, technology specialist in the Office of Technology Integration. “We had a working structure and methodology, and we used it to get our people to address these issues.”

The meetings drilled down to each functional area and its business processes. For example, Angela McCausland, director of ERP, coordinated several sessions with the human resources and payroll staff members to discuss the processes for hiring people, paying them, and recording their time. “I can’t say we captured the entire enterprise, but we did document a big chunk of it,” states Morgan. “The meetings enabled us to delve into all the business processes throughout the organization and get a good inventory of all the pieces.”

The outcome was a spreadsheet containing each functional area’s business process recovery time objectives and recovery point objectives. “We established the time requirements and functional dependencies to understand the system and application dependencies,” states Lazor. “It was a domino effect. For example, you need to process paychecks, but what does this mean? What are the other systems that provide upstream information in order for that to happen? That became the OTI requirement parameter: What are the applications that need to be up by a certain date?” Table 1 outlines FSU’s top 10 functional area/business process priorities identified by the BIA project.

“Even within that context, we still had to make certain decisions about the functionality and supporting systems that we use,” states Morgan. “Our clients understand that. Some of the interfacing systems, as for example the facilities department’s electronic information feed into the payroll system, are not included in this analysis due to cost trade-offs. The department knows that in the event of a disaster, they will have to enter their data manually.”

Just as important was the review of intangible and tangible impacts of a disaster over time. The model enabled FSU to translate a potential disaster’s impact into dollars and cents by calculating the potential costs of intangible items (such as regulatory compliance, stakeholder confidence, and customer service), potential costs of tangible items (such as loss of funding, fines, and emergency purchases), and the financial cost of outage to participating FSU departments over a four-week disaster time frame.

To validate the results, IBM facilitated a team meeting in late August 2005 for all the
Disaster Recovery at FSU  

Table 1. FSU’s Functional Area/Business Process Priorities

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Business Process</th>
<th>Recovery Time Objective</th>
<th>Recovery Point Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time and labor/help desk</td>
<td>Customer service</td>
<td>2–4 hours</td>
<td>N/A</td>
</tr>
<tr>
<td>Payroll processing</td>
<td>Customer service</td>
<td>8–24 hours</td>
<td>N/A</td>
</tr>
<tr>
<td>Student financial services</td>
<td>Tuition &amp; receivable collections</td>
<td>24–48 hours</td>
<td>No data loss</td>
</tr>
<tr>
<td>Student financial services</td>
<td>Financial aid distribution</td>
<td>24–48 hours</td>
<td>No data loss</td>
</tr>
<tr>
<td>Student financial services</td>
<td>Cashiering transactions</td>
<td>24–48 hours</td>
<td>No data loss</td>
</tr>
<tr>
<td>Registrar—student service</td>
<td>Student records management</td>
<td>24–48 hours</td>
<td>12–24 hours</td>
</tr>
<tr>
<td>Registrar—curriculum support</td>
<td>Curriculum management</td>
<td>24–48 hours</td>
<td>12–24 hours</td>
</tr>
<tr>
<td>Finance &amp; accounting</td>
<td>Employee payment</td>
<td>24–48 hours</td>
<td>12–24 hours</td>
</tr>
<tr>
<td>Sponsored research services</td>
<td>Set up award projects for spending</td>
<td>24–48 hours</td>
<td>12–24 hours</td>
</tr>
<tr>
<td>Sponsored research accounting services</td>
<td>Completion of award setup process</td>
<td>24–48 hours</td>
<td>12–24 hours</td>
</tr>
</tbody>
</table>

participating groups. An executive session in the fall enabled middle and senior administrators to review the final BIA results.

Upon completion of the BIA project, OTI and the functional offices struggled with tying all this information together. So OTI purchased a Web-enabled version of Strohl Systems’ BIA Professional software to create a framework and to enable business process owners to access, administer, and integrate the BIA project results into their own dynamic planning. Eventually the participants produced a project document, Disaster Planning Guidance.

The BIA project produced two major results:

- The functional areas discovered the gaps in their business continuity and disaster recovery planning. Angela McCausland said, “There were a lot of gaps that were never discussed. For example, if we did not have a method to get our files to our vendors, what would we do? After every meeting, the participants would go back and talk to their colleagues to determine how to handle these situations.”
- No procedure existed to guarantee production of a payroll in the event of a disaster, so FSU has created an emergency procedure for authorizing its bank and benefit providers to rerun the most recent payroll and benefits file if the system cannot be restored before the next payday. This solution serves most of the FSU population, and it created a stopgap measure in the event of a longer-than-expected payroll process restoration.

FSU built a business case for the benefits of business continuity/disaster recovery efforts. The project created a tangible price tag stemming from a disaster, helping senior administrators
to weigh the pros and cons of implementing the remote disaster site.

BIA project participants believe other institutions could complete a similar exercise. “From a university perspective, the priority order of business processes would be broadly generic,” Morgan believes. “Most institutions would have several similar business functionality priorities, as we do.” Some outside help may be needed, however, for project management and to facilitate the team meetings. “We didn’t know how to complete a business impact analysis in the first place,” states Michael Barrett, assistant vice president, Office of Technology Integration. “You need an active project manager to keep the project moving, to define the goal and the time frame. Without that, the project would drift apart and not meet deadlines.” Project participants also recommended purchasing a commercial BIA software tool to provide an information-gathering, organizing, and reporting framework.

**Hurricane Katrina Provides the Call to Action**

FSU’s dependence on reliable IT services grew in tandem with its increasing dependence upon ERP and course management systems. As a result, “OTI invested significantly in local fault tolerance, redundancy, and failover for our ERP system and some redundancy for our CMS,” states Baker. But work still needed to be done. OTI conducted a pilot to test the feasibility of restoring tapes from its PeopleSoft system onto repurposed high-performance servers and realized that the restoration time was far from satisfactory. “When we started out, I thought a remote tape backup would be enough,” recalls Larry Conrad. “The first time we tested, there were problems. But even taking that into consideration, it became very clear that we needed disk-to-disk synchronization for certain applications, such as Blackboard. Tapes are good, but the data needs to be on disks.”

Later in this case study, tests indicated that recovery from tapes took an unacceptably long time for the purposes of payroll and course management systems. Also fueling the need for synchronization at a remote site was the concern that the building that houses the University Computing Services servers and equipment was not designed to withstand major hurricane-force winds.

Then came Hurricane Katrina in late August 2005. Tallahassee has experienced glancing blows or tropical storms, but no direct major hurricane hit in 20 years. Coincidentally during the IBM-facilitated BIA validation meeting, the conference room’s TV monitor broadcasted a local weather forecast illustrating the hurricane’s projected storm path directly over Tallahassee. When Conrad saw the projected storm path, he experienced what he calls his “ah-ha” moment. “I realized we were not ready for this,” he recalls. “We had done what most people had done for years to prepare for a disaster—for example, backing up critical files offsite. But when I faced the prospect of what would happen if a hurricane of that magnitude hit our campus, I realized that we had to take this type of threat more seriously.”

Hurricane Katrina altered its course, bypassing Tallahassee, and it altered Conrad’s thinking, too. “My view shifted from ‘what to do if we got hit by a hurricane,’ to ‘what to do when we got hit by a hurricane.’ This fundamentally changed the value proposition for me. I realized OTI needed to assemble the financial and managerial resources to tackle the issues of secure backup of data and business continuity head-on to be adequately prepared by the start of the 2006 hurricane season.”

The multimillion-dollar investment in the ERP system, the BIA, and an active hurricane season promoted prompt funding for the project, financed jointly by the university and OTI’s recurring budget. Also instrumental was the immediate executive support for the initiative.
Provost Abele, a longtime supporter of IT, readily provided institutional support, involvement, and financial commitment for the project.

Solution Selection

Having set the priority, goal, and time frame, OTI’s next step was to devise a solution for remote backup as well as business continuity. First, OTI investigated reciprocal space/backup arrangements with Florida LambdaRail sister institutions, but the regional nature of hurricanes nixed that alternative. One hurricane could easily sweep through Florida, disrupting Miami’s Florida International University, Orlando’s University of Central Florida, Gainesville’s University of Florida, and Tallahassee’s FSU. OTI looked farther inland to institutions in the southeastern United States, but no institution could respond adequately to FSU’s June 1, 2006, business continuity and disaster recovery preparedness deadline.

One thing became apparent: “We wanted to design our disaster recovery strategy ourselves rather than relying on a third party,” states Jeffrey Bauer, assistant vice president and chief technology officer. Three main factors contributed to this reasoning. First was the dynamic environment. “Our environment changes so much that even if you test something, a month from now it is going to be out of date,” states Baker. “It’s tough enough to keep our production boxes up-to-date.”

The second factor was requirements for recovery point objectives and recovery time objectives. As Table 1 illustrates, some of the functional areas’ (such as payroll processing and student financial services) self-determined recovery point and recovery time objectives precluded the time lag associated with the restoration from tape backups at a vendor site. OTI investigated third-party disaster recovery service offerings, but typically those required tapes to be shipped to vendors’ facilities, negatively impacting recovery point objectives. The data would be about a week old, which was unacceptable for some FSU areas’ needs, such as payroll and, surprisingly, e-mail. In addition, the BIA illustrated the increasing financial impact of disrupted business operations on the university, prompting the areas’ desire for a swift resumption.

Finally, there were the high-bandwidth requirements. When OTI decided to implement a disk-to-disk synchronization plus backup solution, an evaluation of the amount of data to be transferred made high-speed networking the only feasible option. Luckily, FSU is a founding member of FLR, Florida’s statewide high-bandwidth research and education network, which provided the opportunity to leverage a 10-Gbps networking infrastructure in a creative way. FLR participates in the regional Southern Light Rail (SLR) component of the NLR initiative. “In the past there was not an economically feasible way to go off campus,” states Baker. “We may have been able to create a cross-campus solution using our internal infrastructure, but it would never have been cost-effective for us to implement a solution in another state, hundreds of miles away. The FLR and the SLR give us the opportunity to provide the remote services cost-effectively.”

Admittedly, a regional or NLR high-speed connection may not be available for every institution. “The key, however, is how much data you want to move and how often,” states Kenneth Hays, network specialist in the Office of Telecommunications Networking. “If you’re only moving 100 gigabytes a day and you want to implement an OC3/155-megabits-per-second solution, then you’d be fine.” (See the section “Transportability to Other Institutions” for more information about relevance to other institutions.)

“We realized an OTI-managed solution was a bit of risk because disaster recovery and business continuity became our responsibility,” states Baker. “We can’t blame anyone...
else if it is not ready. But we gain flexibility; we know that the resource will be available for us when needed, and it will be as current as we maintain it.”

Then OTI investigated third-party colocation hosting services. “One of our early designs was to split our development environment from our production environment and to run one or the other out of the remote site, switching over in the event of a disaster,” states Baker. “That, however, would have required us to rent a larger remote site, to maintain a much larger environment, and to have systems that mirror our production system and online storage.” By taking advantage of new blade server technology, eventually OTI chose to operate a smaller, production environment at a remote site focusing on data backup and business continuity purposes for identified critical functions only, requiring a smaller footprint and thus generating lower costs. “Not everyone could do everything they wanted all at the same time, but the essential people could maintain the critical systems during a disaster,” continues Baker.

OTI issued a request for proposal containing the following criteria:

- Low risk of natural disasters. OTI wanted to locate its remote site in a hurricane-free zone, and it did not want to swap one risk for another, such as earthquakes or floods.
- Connectivity or access to the FLR/NLR. This was a primary requirement that would enable FSU to leverage its participation in the FLR to connect directly or via the NLR to back up data to the remote site.
- Compliance with National Institute of Standards and Technology standards. FSU received bids from as far away as New York, Chicago, and Houston, but the cost of networking was prohibitive in some of those areas. “We wanted something that was far enough from harm’s way, from the type of disaster that is likely to hit us, but close enough that we could get to it in a timely manner,” explains Baker. “In our case, it all came together in Atlanta.”

OTI ultimately chose a peering, aggregation location in Atlanta, which “already has the electronics in place to provide an off-ramp for our data to our remote site,” explains Baker. “It was potentially a cross-connect between a peer’s patch panel and our patch panel to get a 10-gigabit connection. Though we are using one cumulative gigabit out of the network now, we have the mechanism in place to go as high as 10 gigabits. This location provides access to high-bandwidth connectivity really economically.”

Figure 1 illustrates the FSU OTI disaster recovery solution for selected processes in its ERP, CMS, and e-mail systems. It illustrates individual 1-gigabit connections from the NWRDC to handle FSU’s ERP data backups and from the OTI site to handle backups for the remaining systems. FSU connects directly to the FLR in Jacksonville, Florida, and then switches to the SLR up to Atlanta. The remote site is tied into a firewall, and data is encrypted and funneled to the site through virtual private networks (VPNs) and virtual local area networks (VLANs).

Currently OTI backs up its data locally using IBM’s Tivoli Storage Manager and completes a remote volume copy to Atlanta each night over the course of several hours. Current volumes range from 2.5 to 3 terabytes per day, of which approximately 1 terabyte is e-mail. In addition, there is disk-to-disk synchronization for some of the critical data sets—for example, those underlying CMS applications, Lightweight Directory Access Protocol (LDAP), and directory services.

OTI maintains no staff in Atlanta. Baker and system administrators update the system remotely when they can, making the 4.5-hour drive only as necessary. OTI outsourced rack construction and equipment installation to a third-party vendor rather than deploying OTI staff and backfilling their positions during
the several months of installation. FSU is addressing the site staffing requirements in the event of a disaster, as discussed further under the “Next Steps” heading.

**Operational Issues**

With the disaster recovery site selected, OTI began the installation process. Most of the hardware arrived in April 2006. The operating systems and applications were installed in May, and backups were flowing by June 1. Finally, the functional staff had to test the remote version of the human resources and financial systems. The disaster recovery site was fully operational by mid-June 2006—at the beginning of the hurricane season—despite the project’s unexpected complexity. “I remember thinking at first that this will be simple,” recalls Bauer. “We’ll take last year’s technology and install it at the remote site. However, once you get under the covers, there are a lot of complexities here. The idea of having a remote site sounds great, but the devil is in the details.” When designing and
implementing its remote site solution, OTI had to address several issues.

**Minimizing Required Floor Space**

The small available space led to a downsized remote disaster recovery site. OTI’s older equipment tended to be bigger, eating up valuable square footage, and it also required more maintenance. “We had to be concerned with the amount of floor space, the footprint, and the power consumption,” says Baker. “These issues precluded us, for the most part, from using equipment that was no longer used in our production site here in Tallahassee.” OTI furnished the remote center predominately with new computer equipment. Another “fundamental problem was plugging all that into a relatively small footprint,” states Randy McCausland. OTI moved to a blade center platform at the remote site to handle many of their Windows, UNIX, and Linux needs, and they used VMware architecture to virtualize as many systems as possible.

**Critical Function Identification**

“Business continuity and disaster recovery are the ultimate ruthless prioritization,” states Conrad. “You can’t afford to do everything remotely. You need a context; you can’t throw darts.” Serendipitously, the recent BIA project provided direction, enabling OTI to determine the required data and systems to support the most critical business functions and processes.

**Mixed Operating Systems, Common Backup**

The disaster recovery solution must address a multitude of complexities, including servers located at both the NWRDC and OTI sites that use Windows, Linux, AIX, or Solaris operating systems. OTI implemented IBM Tivoli Storage Manager for backup and disaster recovery because of its support for multiple clients. “Tivoli is great for backing up files. When it comes to providing the server support for disaster recovery, it is ideal because it touches everything,” explains Baker. “We have so many people involved: the system administrators, the SAN [storage area network] specialists, the database groups, as well as the administrative and academic computing areas.”

**Hot Sites for Critical Systems**

OTI does disk-to-disk synchronization for some of the critical data sets—for example, CMS applications, LDAP, and directory services. “While the servers here are backed up using Tivoli, it is also true that there are genuine hot standbys at the Atlanta site,” explains one OTI staff member. “The database catalogs are rolled forward every 15 minutes on a periodic basis to keep them up to date and to minimize the content delta so the new as well as changes are recorded on the hot standby as well.” The CMS database is synchronized every 15 minutes; application servers are synchronized every hour.

**Cost-Effective Data Storage**

“Our original plan was to operate storage area networks in both Tallahassee and Atlanta, involving special switches to link the SANs to provide a more synchronistic environment with our remote site,” states Bauer. “This, however, can be very expensive. Instead, we devised a lower-cost solution that uses a standard network connection. The data is backed up in Tallahassee and copied as a separate operation to the remote site over the standard TCP/IP network, eliminating the SAN interconnectivity.”

**Optimizing Bandwidth**

OTI had to tune the network to transmit larger data packets to take advantage of the high bandwidth, enhancing its throughput. “We are seeing 800–850 megabits out of the 1-gigabit connection, which is a more efficient use of a TCP/IP connection,” notes Bauer. “If we hadn’t done that, the solution would be inef-
ffective because we would not be able to keep up.” This process involved tweaking buffer size, operating systems, kernels, and applications.

**Domain Name Service (DNS) Resolution**

“We used some interesting tricks with the domain name server to minimize the resolving Web site changes quickly,” states Bauer. “We use the views part of DNS, so depending on what network and view you’re in, you will see something different. Someone who goes to <www.fsu.edu> may unknowingly go to the Web site hosted by the remote site.” An Office of Telecommunications network specialist makes the switch once a senior administrator authorizes the changeover.

**Excessive E-Mail Volume**

E-mail is a critical communication application during a disaster, so this service is replicated at the remote site. OTI backs up the contents of the three FSU e-mail systems daily to record changes to the users’ in-boxes in case a disk fails. This results in a terabyte of data, and the volume is growing. OTI, however, is implementing a new e-mail solution that will store the mail differently and result in a lower volume of data.

**Remote Administration**

To limit OTI’s on-site maintenance requirements in Atlanta, technicians installed a virtual keyboard and video remote console that operates over a TCP/IP or regular phone line interface to gain access to the computer equipment. The department also contracted with the Atlanta colocation company to provide “remote hands” for occasional maintenance, such as cable installation.

Interestingly, Baker identified power as the most expensive operational cost at the Atlanta site. “We thought the floor space would be more expensive, but when you install a very tightly packaged solution like a blade center, it requires significant power and cooling.”

**Next Steps**

Faced with a time frame of less than a year to implement the Atlanta remote site, FSU focused its resources initially on the technical requirements to meet this goal. With the site now complete, FSU is tackling a host of underlying policy and operational issues. The institution is looking for ways to leverage its investment, too.

For example, FSU has to define when it is even appropriate to switch over to the remote site. Activating the Atlanta facility as a remote production site is not a decision to be made without due consideration. “Just because you have a remote site, you definitely do not want to pull that trigger prematurely,” states Conrad. “It would take an extensive disaster for FSU’s buildings to be out of commission for an extended period. So we have to determine if the decision is worth the potential travel time to Atlanta as well as the potential downtime to reinstate our Tallahassee facility after the disaster. We’re still defining that trigger point.” The consensus is that the switchover decision is an executive one, but as an OTI staff member notes, “To help senior administrators in creating this policy, we need to give them a technical briefing about the ramifications for pulling the trigger—for example, the challenges and lag time before the remote site is functional during the disaster, and restoring the local OTI systems post-incident.”

Now that the broader strategic issue of prioritizing business function recovery is resolved, units are working out procedural details at the departmental level. This includes informing the business process owners about the switchover decision, arranging for OTI and administrative department staffing during the disaster, and establishing operational and communication procedures for the business functions and OTI during the remote site’s activation.

Operational issues revolve around equipment and staff readiness. A complicated task is the coordinated testing of the twin hosting
site environments—OTI and NWRDC facilities—to maintain flexibility and readiness in response to various disaster scenarios, which may result in the loss of either or both of the NWRDC and OTI data facilities. Even though each facility maintains a different disaster recovery solution, the hope is to conduct joint testing in the future. The NWRDC completed a successful test at IBM’s Sterling Forest facility in spring 2006 prior to the OTI Atlanta site’s implementation. OTI completed its first tests at the Atlanta site during the following summer to validate that it was active and that users could use it remotely. “We’ve proven it works, but we have not proven we can do it under fire within a two-day window with just one day of data loss,” states Baker. This is especially significant for meeting the BIA project goals in terms of recovery time and recovery point objectives. Another round of testing is scheduled upon completion of FSU’s ERP system upgrade in late 2006.

Just as important is the creation and maintenance of appropriate documentation for the remote site—for example, site diagrams, operational instructions, and maintenance procedures—in a central information repository such as a Web site to which staff members can refer, especially during a crisis. Keeping them up to date is important, too. As one OTI staff member observed, “During the testing you need to keep your notes for use as the basis for your disaster recovery procedures, to identify which parts work, which parts need improvement. Every time you test, your documentation needs updating.”

Work is afoot, too, to leverage the remote site in other ways at FSU. For example, Provost Abele has outlined concerns with data backup in general at FSU. “On a big campus like ours, it is so hard to keep little systems from developing independently,” Abele explains. “We’re trying to discourage autonomous servers that contain critical data; to encourage faculty and researchers to back up their course material and research data on a weekly, if not a daily, basis to protect their data; to prevent any course material from migrating off of the FSU course servers; and to comply with state and federal inventory requirements regarding laboratory and research materials and animals.”

OTI has proposed a suite of services with varying levels of local autonomy that address Provost Abele’s concerns head-on:

- **Automated backup.** A currently available service permits departments to store selected files on a network-attached storage device that is backed up automatically both locally and at the remote site. This eliminates departmental backup requirements for the selected files, and staff members needn’t learn to use the Tivoli Storage Manager protocol. The service costs $15 per gigabit per year.

- **Autonomous backup.** A planned service would enable a department to maintain its own Tivoli server to directly back up files locally or to the remote site.

- **Business continuity services.** Also on the drawing board is the possible placement of departmental servers at the remote site for their business continuity purposes. OTI will not provide any business continuity services; rather, the department would utilize the high-speed network connection to the remote site. A department can choose the level of service on the basis of its need and technical capabilities.

OTI has begun to introduce its capabilities to local departments, meeting with the council of deans and technical support staff members to explain the remote site’s capabilities. Baker is working on a pilot program with four departments to build user testimonies, and he is meeting proactively with likely candidates for the new service offerings.

Finally, there is the introduction of the remote site concept to other higher education
constituencies. A statewide disaster recovery/business continuity initiative following OTI’s concept is under consideration, too. Florida’s board of governors, which represents 11 higher education institutions in the state, has created an emergency management task force to gather institutions’ experiences around the state. The task force has approved conceptually a proposal to create a similar statewide solution using the FLR. In addition, OTI wrote its original contract with the Atlanta colocation site in such a way that other state institutions, including smaller ones, can piggyback on FSU’s contract without a new request for proposal. Each institution would submit a request for quotation for pricing to suit its requirements. In a related initiative, FSU, the University of Florida, and the University of Central Florida are investigating how to keep their institutions functioning academically during a crisis. Blackboard offers chat functions and other capabilities to promote distance learning, but the three institutions are exploring ways to perhaps post content and recorded lectures on the CMS, which in turn could be stored at a remote site.

**Benefits and Challenges**

The remote site offers numerous benefits. The most obvious is that FSU now has for its critical functions a remote backup and real-time business continuity capability outside the Florida region hurricane zone. The next time a hurricane threatens the Tallahassee area, OTI has the option to switch over its operations if appropriate. The facility is available to support FSU in other crisis situations, too.

Other benefits have emerged. For example, there is increased awareness about the importance of business continuity practices outside the OTI organization. The BIA educated the business process owners about the true impact of a disaster on their operations, creating a partnership and buy-in with OTI on the remote site project. The business owners determined their recovery point objectives and recovery time objectives, the applications or dependences related to those goals, and the impact on institutional image or loss of revenue within specific time frames. This enabled all parties to ask the provost collectively to fund the remote site.

For OTI, the remote site’s design process “forced us to peer under a lot of ‘rocks’ that we hadn’t looked under for a long time,” states Baker. “It caused us to increase our coordination on backups and to review our applications and systems and decide which ones are really important.” The remote site, too, provides “a nice playground for OTI to test fire-walling, blade technology, and virtualization without impacting our production environment,” states Bauer. It has broadened the staff members’ technical expertise.

The remote site presents several challenges, too. During implementation, OTI faced the issue of using outsourced or internal resources. OTI did outsource parts of the disaster recovery site’s implementation, but it was not a panacea. It did save time and travel, but some of the work had to be redone. “Outsourcing the operating system installation did indeed provide value and shortcut some of the tasks that we could have completed internally, but we still found ourselves having to work and correct issues,” states one OTI staff member. “There was more time investment on our own side of the house than we guessed initially when we decided to outsource the installation.”

Manpower issues may loom, especially if staffing resources become tight. The remote site added another dimension to every system administrator’s job, as there is another site to maintain for every software patch, upgrade, and implementation; or, as Baker concedes, “The disaster recovery responsibility was tacked onto our people’s existing jobs.”

Another ongoing battle is with complacency. Two very active hurricane seasons in 2004 and 2005 mobilized FSU’s support and implementation for the Atlanta remote site.
With a relatively quiet 2006 season, “there is the challenge of maintaining the motivation and discipline to keep this initiative going,” explains Morgan. “Some of the emotional intensity has abated.” If the trend continues for three or four years, it may be difficult for disaster recovery to maintain its priority, especially when competing against other OTI priorities for financial resources. If quiet hurricane seasons continue, the temptation becomes great to utilize the remote site for more than disaster recovery, especially to help justify its operation if budgets are tight. But OTI has to tread warily in this direction, for, as Baker observes, “If you start to depend on the site too much for normal operations, it is no longer disaster recovery.”

Last, but not least, is the issue of recurring funding. As the disaster recovery site implementation was funded primarily with nonrecurring funding, it is not obvious where its future funding will originate. “This needs to be built in on the front end with ongoing costs,” states Michael Barrett, OTI assistant vice president. “OTI and the business areas are struggling with how to effectively build in the cost infrastructure.”

Lessons Learned

Members of the FSU community offer several lessons learned: some are general truisms; others are specific to business continuity and disaster management practices.

- Don’t get mired in details when implementing a disaster recovery site.

Speed was essential for OTI to implement its remote site in several months before the subsequent hurricane season began in 2006. Consequently, Conrad and OTI did not dwell on many nontechnical details in advance, focusing instead on the expeditious business unit and senior administration buy-in. This provided project direction and political support, but OTI tackled many of the policy and procedural details after the remote site’s implementation.

- Business continuity technology decisions should flow from user business decisions.

“The process did not start out with technology,” states Morgan. “It started with the business office staff members peeling off layers of the onion to work down the organization in order to understand their key business responsibilities and functions and their recovery priorities. Only after this process was completed could OTI review technical solutions and consider the cost aspects.” Involving the users dispels the notion that disaster recovery is just an IT function. “Having IT take care of data is not a disaster recovery plan,” states Baker. “Everyone needs to understand their role in providing business continuity in case of a disaster. You can’t assume that IT will take care of it.”

- Focus on the core set of services when determining the disaster recovery site’s capabilities.

OTI supports numerous institutional functions and processes, but “you want to concentrate on the essential services, not to be all things to all people, to keep your solution doable and attainable without costing too much,” states Baker. The BIA and executive involvement provided guidance in this area.

- Do a BIA to create an objective prioritization of services to be handled by the disaster recovery site.

“I freely admit that I was initially ambivalent about the BIA analysis, but after the fact, I am convinced it was worth every penny,” states Conrad. “It created a structure and methodology for our people to address these issues.” The study was invaluable in creating a business case to justify FSU’s investment in the remote site, and it provided guidance for prioritizing which systems to support at the remote site. “It forced a consistent ordering of thoughts across different functional units that allows the disaster recovery team to put apples to apples.
and oranges to oranges,” states Rick Burnette, associate director, Office of Admissions.

- **Disaster recovery is not a financial afterthought; plan for ongoing funding at the project’s inception.**

“Disaster recovery is a part of the cost of doing business,” states Barrett. “You need recognition of it from a budgetary viewpoint up front, or you’ll be scrambling as we were to convince people to fund this project.” Barrett further recommends setting aside a certain percentage of every system investment for disaster recovery protection as an insurance policy. “It needs to take place shortly after you implement the new system or you will get caught in a cycle of ‘now it is a new requirement and we need to find new funding.’ Some institutions would struggle to find the money after the fact.”

- **But designing an application or system backup in the event of a disaster should take place after the fact.**

OTI discovered an interesting finding through its experiences: It is not feasible to design a backup concurrently with an application, system, or database implementation. “The reality is that it does not work that way,” states an OTI staff member. “You must program and bring up the systems, enhance them, and stabilize them before you understand how the system operates. It is a follow-on activity.”

- **Factor in ample time for a disaster recovery/business continuity implementation, as it does not happen overnight.**

“We started out with a very simplistic idea as to what it would take to implement the remote site: test older equipment and ship it to Atlanta,” acknowledges Morgan. “We estimated it would take a year for completion, but it is not that easy. Finding the time to work on it in conjunction with our other duties, the learning curve involved, testing, and now creating relevant documentation for procedures…it has turned into a two-year project.”

---

**Transportability to Other Institutions**

Most organizations will resonate to the disaster recovery utility of the near-real-time remote synchronization of data and the ability to quickly reestablish operations at a remote location such as FSU has developed. However, some may feel that FSU’s circumstances might be relatively unique—being in a hurricane zone, having access to the regional LambdaRail, and so forth—yet this model is relevant and transportable to other institutions.

**Drivers**

Independent of being located in a hurricane zone, every institution, according to current conventional wisdom, should have critical disaster recovery capabilities at least 50 miles from the usual operations center. The *Post-9/11 Emergency Response and Business Continuity Changes at Pace University and New York University* (Metz & Spicer, 2007) and *University of California, Davis: Creating an Institutional Framework for Business Continuity* (Albrecht & Pirani, 2007) case studies that also complement the ECAR research study on business continuity, *Shelter from the Storm: IT and Business Continuity in Higher Education* (Yanosky, 2007), document other disaster scenarios that could occur and require the same level of response as FSU has developed.

**Implementation**

The key to effective and efficient implementation of a near-real-time remote location is embedded in the BIA: What are the critical business processes that require continuity of operations in the event of a major disaster; in which priority are these processes arranged; and what are the operational recovery time objectives and recovery point objectives?

Having established this framework, one can then develop a model that can inform the network infrastructure requirements to
support remote data synchronization. Smaller, less complex institutions than FSU may well find after this analysis that commercially available network services could suffice. After this, it becomes a matter of replicating what you can afford to replicate.

Of course, as FSU discovered, there are staff implications, which could be a significant ongoing cost. As discussed above, FSU did a combination of contracting for basic tasks and adding to the load of regular staff. While adding to the staff load has clear negative implications, FSU did find that it also allowed staff to improve normal operations and gain some long-term efficiencies.

**Conclusion**

Baker notes, “We started this initiative for two reasons—not just for disaster recovery but also for remote secure backups of data. You can always get machines, but the data is very hard to replace. We identified all of our critical systems and got them in a common backup method. Now we have current backups of all critical data, in Tallahassee and Atlanta.” This was a significant driver for FSU to undertake a do-it-yourself strategy. Having previously invested in the necessary networking infrastructure has allowed FSU to implement this strategy in a very substantial manner.

**References**

