Lemons to Lemonade:
Disaster Preparation and Recovery

Jenifer Jarriel, Baylor College of Medicine
Charles R. Shomper, University of Houston
Overview

Water, water everywhere—that was the problem in Houston, Texas, in early June 2001. Tropical Storm Allison, the first named storm of the 2001 Atlantic hurricane season, struck the Houston area over a five-day period, dropping nearly 37 inches of rain in the Port of Houston. By the early morning hours of Saturday, June 6, it had produced catastrophic floods in Houston and heavy rainfall and flooding as it continued from Louisiana to North Carolina and then northward along the east coast to Massachusetts. The Federal Emergency Management Agency (FEMA) reported that damage in the Houston metropolitan area alone totaled approximately $4.8 billion, and almost half of that represented damage to public facilities, particularly the Texas Medical Center. In some areas, colleges and universities in Houston reported water accumulation up to 10 feet, causing tens of millions of dollars in damage to buildings, infrastructure, equipment, research, and irreplaceable archives. Parts of Harris County, in which Houston is located, experienced what is referred to as a 500-year flood, which has only two-tenths of one percent chance of occurring each year.

Figure 1. Exterior of Baylor College of Medicine After Tropical Storm Allison

Naturally, organizations hope that a disaster of this magnitude will never strike, but it is clear from this event, the events of September 11, 2001, and other disasters that disasters do occur and will impact our institutions. While nothing can better equip an institution for a disaster than living through one, prudent preparation and recovery plans are a necessary and important part of business continuity planning. Planning is also valuable for dealing with what the Business Continuity Institute refers to as “quiet
catastrophes”—those that have the potential to damage your institution’s most valuable assets, including its brand and reputation.²

**Figure 2. University of Houston Law Library After Tropical Storm Allison**

This research bulletin explores how two Houston higher education institutions—the University of Houston (UH) and the Baylor College of Medicine of the Texas Medical Center—recovered in the aftermath of Tropical Storm Allison by applying a foundation of good practices and by developing a set of principles to help with disaster recovery and prevention. Specifically, it addresses the role that information technology (IT) and the IT leadership and staff played in campus-wide recovery efforts and the refocusing of institutional priorities in response to the Allison disaster. Because many of these principles and practices are generic in nature, they can be applied to other institutions and to continuity planning for different types of natural and man-made incidents.

### Highlights of Disaster Preparation and Recovery

McMillan and Sitko³ said that effective preparation for unimaginable incidents that disrupt university life is one measure of an institution’s awareness of the risks it faces. As early as 1997, the Massachusetts Institute of Technology (MIT) developed a business continuity planning tool that addressed the campus’s increasing dependence on computing and communication resources for maintaining continuity in the event of a disaster. This Functional Area Recovery Management (FARM) Team plan⁴ is a tool to help MIT schools and departments prepare for incidents that could make IT resources
unavailable for short or extended periods of time. It includes incident classification criteria, principles, procedures, and practices that are still valuable today.

Although no one can predict how a catastrophic event will affect an institution or the specific recovery mechanisms that will be required, institutions that have recovered from such incidents attribute much of their success to wise investments, rational structures, good practices, and lucky breaks.\(^5\)

For this research bulletin, ECAR interviewed Jenifer Jarriel, vice president for information technology and chief information officer at the Baylor College of Medicine, and Charles (Chuck) Shomper, former vice president for information technology at the University of Houston, to learn about the strategies, structures, and resources that their institutions employed during the recovery from Tropical Storm Allison.

### Risk Awareness

**ECAR:** Can you briefly describe what happened on Saturday, June 9, 2001?

**Shomper:** At about 3:00 a.m., the associate vice president for computing and telecommunication services got a call from our chief IT network engineer who was on campus upgrading the voice mail system. The engineer reported that his staff had to evacuate the central IT computer center building because it was flooding quickly. By 6:00 a.m., I notified the chancellor that the situation was dire, and by 8:00 a.m., as the AVP and I drove to campus to gather supplies and begin work on recovery, some interstate highways and nearly all access roads that led to the campus were flooded. Fortunately, by then a few key IT staff members had arrived on campus, joining the staff members who had been there the night before. We secured flashlights and rubber boots, and these turned out to be some of the most valuable survival gear we had. We also gave cell phones and pagers to everyone who needed one, knowing that we would be scattered across campus as emergency rescues began. Institutional priorities were, of course, focused on saving lives. We thought that IT would be concentrating on restoring telecommunications, data, and video network connections, but while we were pumping water out of our key facilities, I redeployed IT staff to help save the animals in our science and research building. At that time, the library, which is on slightly higher ground, was still operational.

**ECAR:** What are some of the wise investments your institution made prior to June 2001 and the arrival of Tropical Storm Allison that helped you recover from the disaster?

**Jarriel:** What comes to mind first is that although our data center was not one that we would have showcased, it was extremely fortuitous that it was not located in the basement of a campus building. Over the three or four years prior to Allison, we had been increasing both the capacity and the redundancy of our networks. Because the networks were more resilient, we could tolerate some interruptions. Our rate-limiting resource in the aftermath of the storm was power.

**Shomper:** We, too, were fortunate that our data center was above ground, although some of our key equipment was located in flooded areas below ground. Since our telephone switch was severely damaged, we felt very fortunate to have on hand many
cell phones with paging capability that we could use to communicate with technical staff members who were working in different parts of the campus. We also were able to secure enough cell phones for the campus executives who needed them for recovery work. We had also invested heavily in a disaster recovery plan for Y2K. As part of that plan, we had outlined administrative and communication processes that we were able to call into play during the Allison recovery. Had we not articulated the specifics of those procedures, the campus would have had to make many more ad hoc decisions that, in times of crisis, are not always well formulated.

**ECAR:** What are some of the structures (organization structures, relationships with government and vendors, etc.) that helped in the recovery?

**Jarriel:** When Allison hit, we had in place a campus-wide emergency preparedness structure for executive-level essential personnel. We knew who to call in an emergency, all campus leaders maintained an internal contact list, and we had procedures for setting up a communications command center (also known as a War Room). Key institutional administrators, with the exception of the president, serve as part of a rotation as the administrator-on-call, including vice presidents, the chief operations officer, and the heads of the bio-safety group, human resources, public affairs, development, security, business operations, ambulatory operations, employee health services, general counsel, and information technology. Each of us serves a one-week shift, and we are on call 24 x 7. The administrator-on-call carries a pager and has a manual that includes the work, home, pager, cell, and e-mail contact information for all other administrators. As new people join the team, we have an administrator-on-call in-service training to review the procedures and the contents of the manual. We also use a buddy system so there is always a backup administrator-on-call. The information technology department uses a similar structure, and the administrator-on-call knows which IT people to contact in an emergency.

**Shomper:** We were fortunate to have excellent relationships with the vendors of our equipment and with the university facilities crew. During the days of our recovery, over 100 vendor representatives showed up on site to help us assess the water damage to our equipment, fix what could be fixed, and deploy new equipment as needed. People were empowered to make on-the-spot decisions, and they had the university’s best interests in mind. Many volunteers and the university’s facilities staff worked around the clock, with everyone pitching in to do whatever was most critical. Institutional priorities became very clear, and nearly everyone seemed to be making Herculean efforts to pump water, remove damaged equipment, design and install new systems, and restore power. We all pitched in to find temporary fixes to urgent problems and to develop parallel contingency plans. Suddenly, the normal bureaucracy was completely absent. Because the UH Web site was offline initially, we worked with the local broadcast stations to share news about the status of the university. Some 40,000 students, faculty, and staff were eager to know the conditions on campus, so we did everything possible to get news to them.
ECAR: In terms of investments, structures, and good practices, what was not in place prior to Allison that you wish had been?

Jarriel: Clearly, we needed better flood protection on campus. We are now looking at the issue of creating and establishing what are referred to as 50-year floodplain walls to protect our lower areas. We are also installing submarine doors that can be activated at any time, and we are examining how electricity feeds into the campus. We’re looking at redundant power from different grids. Any activity like this tends to highlight the vulnerabilities you have.

Shomper: Some of the diesel-powered uninterruptible power supply (UPS) systems failed, and we had a challenge getting enough diesel fuel to them. Systems have been upgraded since then, although we know that we are still not fully protected from catastrophe. On top of everything else related to the flood, lightening recently happened to strike a 5-foot line between our diesel generator and our main university center building. The dilemma, of course, is how does one manage to prepare for every risk? Complete risk avoidance is prohibitively expensive.

Risk Assessment

ECAR: How has your campus changed its approach to risk assessment as a result of Allison?

Jarriel: With respect to the risk of flood (for example, our activities prior to 2001), we primarily focused on the use of sandbags. Of course, these wouldn’t have helped much in a storm of the magnitude of Allison. Now we are looking at how to be far more proactive and at how to work with external agencies to find solutions that will benefit not only the campus and the Texas Medical Center but the city at large. We continue to work with FEMA to evaluate and renovate our vulnerable physical spaces. We’re flood-proofing more areas and installing submarine doors where needed. We never realized the risk of having a skylight in the hallway leading to data center, for instance, but we have now closed it in. No critical functions are located in basements or sub-basements any more. A schedule for updating the emergency contact list and the Emergency Response Manual has been established, and a permanent area for food services has been designed. We’re paying more attention to employee health, and have set up an on-site center to handle minor emergencies. We have learned that you cannot assume things will work in an emergency. Cell phones, for instance, do not always work when landlines are down. We are paying attention to the small items: having flashlights and batteries available and visible, battery-backed emergency lights, a battery-powered radio, bottled water, an updated first-aid kit. And we now know how important tetanus shots can be.

Shomper: Prior to Allison, our campus was very concerned with the potential catastrophes resulting from fire, wind damage, and, after the war in Iraq started, terrorism. One giant impact of Allison was that the force of the water was so intense that it broke through windows and allowed the rain to flood the massive tunnel system that connects the buildings on campus. Although information technology has always been included in campus-wide disaster planning efforts, people were so taken aback by what
this storm had done to the IT infrastructure that they became much more sensitive to it. In fact, the storm helped IT’s cause around disaster recovery and redundancy. [Jarriel concurs that when phone and computer services are disrupted, people become very sensitive to IT issues.]

**ECAR:** How does your campus define “essential” IT systems and services that are the first priority in an emergency?

**Jarriel:** Some of the things we thought were most critical were not, and vice versa. For instance, the Baylor Web site had not been considered an essential system, but we learned that it was indeed critical, both for posting announcements and for soliciting information. People needed to know what the condition of the campus was, including whether or not it was accessible, especially once the public media began reporting on the crisis at the Texas Medical Center—no power, accesses blocked, patients being evacuated, and so on. The telephone switch area had to be powered down due to lack of air conditioning and the resulting increase in temperature. We thought that getting our voice service back in service was our highest priority. Other “highest” priorities were e-mail, basic network connectivity, and SAP, most especially for access to our purchasing system. Very soon after the initial crisis was over, we also needed to bring our clinic appointment scheduling system back online. The storm happened to hit us on an off-week for payroll, otherwise that might have been another highest priority.

**Shomper:** Vendors of all kinds were willing to defer payment until our systems were brought back online. This type of superior service and flexibility from vendor partners is only available for a major and generalized disaster. It would have been much more difficult to obtain if the disaster had hit only our campus, such as a fire in our data center. At the University of Houston, critical infrastructure services include our data center operation, Internet connectivity, intercampus network [UH System has four campuses], interactive video network, phone system, and our campus data network. With respect to applications, our most critical are e-mail, the UH Web, WebCT, payroll, financial applications, and services related to registration and records.

### Disaster Planning

**ECAR:** Describe the type of IT disaster plan that was in place prior to Allison and the plan that is in place now.

**Jarriel:** In many ways, our *Emergency Response Manual* was extremely valuable, especially in terms of having current contact information for key individuals. On the other hand, I’m not sure that any disaster plan could have anticipated some of the situations we encountered. For example, we lost use of our master security and alarm system, so we established a 24 x 7 staffing schedule for our computer facilities. We found ourselves installing VPN connections for over 82 individuals and trying to recover data from submerged drives. I doubt that anyone could have imagined the level of devastation from this storm to enable us to have a disaster recovery plan that would have been truly useful.
Shomper: The university basically relied on the disaster plan we had developed for Y2K. Our first dilemma was where to execute the plan, since the place that had been designated as the emergency command center was unusable because the infrastructure systems were damaged in the building [all electronics and power were in the flooded basement]. Once we found an alternate setting for the command center, we realized that some of the contact information we had was out of date. It became clear that having a paper manual that is difficult to keep up-to-date was not the best solution for our contacts list. On the other hand, if we had relied solely on a central electronic database for contact information, that data would have been inaccessible to us in the storm. What is really needed, of course, is multiple “copies” of up-to-date contact data for university administrators and key professionals, including key vendors, which can be accessed in various media, both from on campus and from off campus. It cannot be overstated how important it is to pay vigilant and ongoing attention to keeping your contact information up-to-date and accessible. Although it is probably a bit unrealistic, we also found that it would have been helpful to have a guidebook to help us navigate through the disaster—someplace where we could look up “worst flood of the century” and see a step-by-step guide to what to do! In the early hours of the storm, perhaps what we were looking for was a comprehensive disaster plan that specified what to do in case of flooding.

Incident Management

The U.S. Department of Homeland Security makes available a 152-page document about the National Incident Management System that includes a chapter on communications and information management. Companies build incident management software, and a Web search on “incident management” yields voluminous results. Managing incidents effectively is both a science and an art.

ECAR: In terms of importance and urgency, what were the most vital elements of IT’s response to managing the Allison incident?

Jarriel: With flood waters rising, we urgently needed to get people and key equipment out of harm’s way. At the same time, we had to stay in touch with institution officials, both to alert them to the status of university systems and communications and to coordinate the institution-wide response to the emergency. I think my most important roles were to lead the IT staff toward efficient and effective management of the crisis and to attend to the human impacts of the storm: fear, fatigue, worry, nourishment, and, in some cases, panic.

Shomper: We didn’t have much time to think through decisions. Everything seemed accelerated: we had to act fast, we had to change our priorities quickly and often, and we made what seemed like very quick decisions. Having been focused on IT for so many years, it was a big surprise when campus officials asked me to redeploy all IT staff to save the research animals instead of restoring IT systems. To their credit, the staff members dropped everything, asked no questions, and waded with me into deep water to do what was necessary. I was both grateful for and proud of our staff and their commitment and support.
What It Means to Higher Education

Elements of business continuity and disaster planning, incident management, and disaster recovery are focused largely on the goals of restoring “normal” operations (although most often this is a “new normal”) and on ensuring that the cycle of planning, management, and recovery is perpetuated.

Restoring to the New Normal

ECAR: What did you and/or the campus do to demarcate the end of the emergency and the beginning of “normal” operations?

Jarriel: We were most eager to restore a sense of normalcy by getting students back to class, researchers back to their labs, clinics operational, and university operations online as soon as possible. Despite the fact that many of our facilities were damaged, all our customers needed to know that support of their mission was our highest priority. Additionally, in this particular disaster, we were dealing not only with damage to campus facilities but also with very severe human realities—faculty, staff, and students whose homes were flooded or destroyed; those who were without means of communication or transportation; and those who had lost family and friends, pets, automobiles, and other valuable or irreplaceable property. The cost of this human disaster was enormous, and we set up special programs and services to deal with them.

Shomper: Like Baylor, UH was focused on restoring classes as quickly as possible. Symbolically, we tried to close the official command center as quickly as possible, as a statement that we were focusing on the return to normal operations. Although we could not open some of our campus facilities right away, we reestablished critical services in “dry” locations. For example, our sports pavilion was in good shape, so we set up temporary offices, a computer lab, and an information technology help desk there. We also worked vigilantly to restore services to the campus library, cafeteria, and dormitories. The president also held a formal recognition event to acknowledge the enormous contributions of the entire university community during the disaster. This event took place at the Houston Astros game where Barry Bonds tied the home-run record.
Perpetuating the Cycle

ECAR: What lessons were learned with respect to risk awareness, disaster planning, and disaster recovery?

Jarriel: We learned that we cannot depend upon assumptions. We had assumed, for example, that cell phones would work when landlines were down, and that turned out not to be the case. We also learned to rely on our business partners, not simply for the services they typically provide but for services at all levels. We also learned to pay attention to the small things, like having flashlights available and visible, having battery-backed emergency lighting, having a battery-powered radio, keeping bottled water on hand, and maintaining a fully-stocked first aid kit.

We also learned a wonderful lesson about teamwork. You can have a comprehensive plan, plentiful resources, and engineered redundancy, but when something as significant as a storm like Allison occurs, you understand the true meaning of teamwork. The focus, tireless energy, and true concern for the people and the organization provided the momentum for recovery. Daily, there were awesome acts of "ordinary people doing extraordinary things."

Shomper: We learned that having a comprehensive disaster recovery process that includes up-to-date contact information is essential. We learned that housing key equipment in the basement of buildings is a bad idea, and this includes utility feeds, telephone switches, and computing equipment in general. We also learned that no matter how resilient our voice and data systems might be, without power they are
useless. And we learned that lightening can strike in your most vulnerable spot, even if it’s only 5-feet long!

**Key Questions to Ask**

- In an emergency, how will the institutional leaders communicate with each other? What are the protocols and procedures? How and where will they find an up-to-date contact list? Where should they convene (initial and back-up locations)?
- Which institutional business processes are considered critical with respect to what needs to be restored first?
- How can the institution manage incidents in ways to minimize risk to current operations, future enrollment, and donor support?
- What would happen if the systems that control security and alarms in residence halls, classroom buildings, and administrative facilities are compromised?
- What are the consequences if environmental pollutants make access to campus facilities impossible?
- What would result from the complete or partial destruction of key buildings and the records they contain?
- How will the institution operate in the face of long-term inaccessibility to communication systems?

**Where to Learn More**

- Search on the term “disaster recovery” to retrieve resources from the EDUCAUSE Resource Center, <http://www.educause.edu/search/>.

**Endnotes**

4. Ibid.


About the Authors

Jenifer Jarriel (jenifer@bcm.tmc.edu) is Vice President for Information Technology and Chief Information Officer at the Baylor College of Medicine. Charles R. Shomper (shomper@uh.edu) is former Vice President for Information Technology at the University of Houston.