INFORMATION TECHNOLOGY SERVICES SUPPORT FOR EMERGENCIES

Donald Z. Spicer
University System of Maryland

I. BACKGROUND

For at least the last quarter century, enterprises—including higher education institutions—have increasingly relied on Information Technology Services (ITS) for business functions. As a result, IT organizations have had to develop the discipline of production operations as well as recovery procedures to respond when those operations are disrupted. More recently, both the academic and research mission activities of higher education institutions have become increasingly supported by ITS. That ITS touches almost every activity of a higher education institution puts special emphasis on IT services in emergency situations. This paper outlines an evolution of thinking regarding the role of ITS in enterprise emergency response.

II. HISTORICAL PERSPECTIVE

Historically, IT organizations did Disaster Recovery (DR) planning and testing based entirely on their own needs for continuity of operations. The major risks were fire, flood, power outage, equipment failure, and human error. Plans were driven by self-preservation from the inside and auditors from the outside. Given these risks and drivers, the responses have tended to be operationally focused: save the data at all costs and be able to restore the data center. On the planning front, auditors have almost universally mandated DR plans, and this mandate usually included testing of these plans and training of technical staff. However, most DR plans tend to be highly localized in scope and very procedural—arranging for varying levels of back-up power, management of back-up tapes with off-site storage, and more recently arranging for re-establishing servers at a remote location.

This historical perspective was one that made sure that the institution was protected in the event of an incident that impairs the machine room of the Computer Center. However, while continuity of IT operations is important for higher education institutions, it is not directly mission-related, per se. The aftermath of 9/11, Katrina, and other regional events, has had big impacts on institutional and IT leadership at many institutions, and the historical view of DR is evolving.

III. NEW PERSPECTIVES ON ROLE OF IT IN DISASTER RECOVERY

First, it is being recognized that the issue is not just one of Disaster Recovery, but more broadly one of Emergency Response. While this shift may appear to be a matter of semantics, it is a recognition that institutions need to respond to issues well beyond the traditional ones of flood, fire, power outage, equipment failure, and human error. The emerging concerns of a pandemic, for example, don't readily fall into those categories. Also, what is needed from ITS is now perceived to be well beyond self-survival and recovery of operations. In an emergency, the ability to communicate—internally and externally—becomes a key service for an organization. The organization's website has become the vehicle of choice for general information regarding status of the situation and tactical issues related to a response. Similarly, email and text messaging are more focused vehicles to tie key personnel together. Thus, while

an organization can tolerate several days of business systems unavailability, communication services must have an instantaneous fail-over capability. Telephony would of course be normally prime amongst such services, but sustainability of the telephone service is beyond the scope of capability for most organizational IT services. Also, Katrina and 9/11 have shown the vulnerability of landline and cellular phone systems in regional disasters. The Internet was designed to be redundant and, if properly conceived and implemented, Internet services are more likely to be sustained in such situations.

Further, in a broad scale or long lasting emergency, the issue is likely to be not about reconstituting business services, but on maintaining the mission activities. Thus for higher education, the focus would be how to preserve the teaching, learning, and research programs. Regarding teaching and learning, online learning—which is an Internet based service in most instances—could be sustained more readily than place based teaching and learning, if the delivery system is designed with potential emergencies in mind. Thus, continuing the academic program in the absence of the ability to meet in traditional classroom settings would become one of proper design of supporting infrastructure and services (an ITS responsibility); having faculty and students prepared to teach and learn online; having academic policies that provide the flexibility to accommodate an emergency switch to online courses; and having access to a portfolio of online courses to meet students' needs during an emergency.

If the emergency is truly long lasting, then online versions of various other institutional services—library, advising, financial aid, student accounts, payroll, benefits, and more will have to be available as well.

IV. DESIGNING FOR EMERGENCIES

As the discussion above shows, organizational processes that have redundancy and/or fail-over capabilities are the ones that can be sustained in the event of an emergency. IT organizations have long worried about designing redundancy and fail-over capabilities into their operations. Academic and research programs typically haven't. Not every region is subject to various natural or human generated disasters. One has to set priorities based on perceived risk. Often implementing an initiative or program requires all of the resources that may be available. Investing in the insurance, for that is what it is, of emergency response alternatives, is generally not in the budget.

All this being said, increasingly IT organizations are discussing so-called "resilient architectures," (i.e.,approaches to services) from conception through implementation, take into account the fact that perceived risk factors may make normal service impossible. While disaster recovery has been conceived as a response, resiliency is conceived as much more inherent in the design of the service.

Since online learning is likely to be more sustainable than traditional classroom learning, the resilient approach to sustainability of academic programs would be to build into the normal curriculum the expectation that faculty and students have experience and capability to teach and learn online. Additionally, having a portfolio of core courses that are offered online would allow this offering to be expanded in the event of an emergency.

V. SOME LESSONS LEARNED FROM RECENT EMERGENCIES

- Traditional planning worried about things and business processes. Broad scale emergencies show that one has to focus on people in planning a response. Do people know where to go, what to do, and how to communicate in such an event? If the emergency is long standing, do people know how to continue their work in a new modality?

- Does the institution's administration have plans and has the IT organization operationalized its role if it becomes necessary to create an "administration in exile" when normal facilities are unavailable?
- If your institution doesn't have a crisis but a near-by institution, or the region as a whole, has one, are you prepared to support their needs? Brian Voss of Louisiana State University (LSU) has spoken and written widely about the impact on LSU during Katrina. LSU was largely unscathed, but the campus became an operations center for the National Guard and FEMA. This put huge strain on LSU's facilities and services.

VI. CONCLUSION

Many of the activities in higher education now depend on Information Technology. Thus, at every higher education institution, ITS will perforce play a key role in any Emergency Response plan and implementation. Recent events and possible future events (e.g. a pandemic) have been a wake-up call for institutional leadership and particularly for institutional IT leadership. The scope of emergencies has increased and the understanding of appropriate responses is also changing. IT leaders are recognizing that business continuity means continuity of the enterprise as a whole.

From the perspective of the online learning community, these trends should be good news. Online learning is becoming recognized as a component of a response to large-scale emergencies. Online learning, however, depends significantly on infrastructure architected, implemented, and supported by institutional ITS departments. That the leadership of these departments recognize that continuity of the academic program is in part a component of their responsibility is an important step in the success of such program continuity.

VII. ABOUT THE AUTHOR

Donald Z. Spicer is an ECAR senior fellow, and the CIO and associate vice chancellor for Information Technology for the 13-institution University System of Maryland. He has previous experience as a faculty member and as an academic administrator. He previously held CIO level positions at the University of Notre Dame and Vanderbilt University. He has made contributions to EDUCAUSE, serving as chair of the Current Issues Committee, program chair of the inaugural Mid-Atlantic Regional Conference, and as a member of the Core Data Service Research Task Force and the 2005 Annual Conference Program Committee. His recent publications include a chapter in *The Wired Tower: Perspectives on the Impact of the Internet on Higher Education*.

VIII. SELECTED FURTHER READING

1. LSU CIO Brian Voss. http://www.educause.edu/LibraryDetailPage/666?ID=ENT06019.
2. Chronicle of Higher Education Compendium. http://chronicle.com/indepth/katrina/.
3. Flu Wiki. http://www.fluwikie.com/pmwiki.php?n=Main.HomePage.
4. CDC Planning Guides for Educational Institutions. http://www.pandemicflu.gov/plan/tab5.html.
5. Univ of California System Plans Post-Katrina. http://www.educause.edu/ir/library/powerpoint/WRC0675.pps.