

EDUCAUSE Center for Applied Research

Research Bulletin

Volume 2007, Issue 20

September 25, 2007

Changing Ideas of Campus Disaster Recovery: Designing Resiliency into Systems

Suresh Balakrishnan, University System of Maryland

Robert "Rob" Sapp, University of Maryland University College

Eric Spangler, University of Maryland University College

Donald Z. Spicer, ECAR and University System of Maryland



Throughout its 60-year history, the University of Maryland University College (UMUC) has been a progressive provider of higher education in nontraditional and evolving academic environments. From holding face-to-face courses in military conflict zones such as Bosnia and Afghanistan to offering distance learning in locations as remote as Antarctica, UMUC has built its reputation on adapting to the needs of its students and using available resources to accomplish its mission. Over the past few decades, the progression of technology has offered UMUC the opportunity to make education available to the nontraditional student using a variety of technologies, including virtual classrooms, interactive video networks, and, in the early days, courses heavily dependent on voicemail. With continuous adaptation to a changing landscape of both technology and business requirements, the importance of building resilient systems from the fabric of technology, people, and business practices grows increasingly critical.

The purpose of this research bulletin is to suggest a framework to provide resiliency in higher education by placing such considerations up front in the evaluation, selection, and design of information technology (IT) services and building them into the business practices of the organization. Resiliency is the product of technology, people, and processes that minimize the impact of an event and make transparent that which would otherwise adversely disrupt the normal operation of services for students, faculty, or staff.

The adoption and now commonplace use of “always on” services on the public Internet has increased the same expectation among students, faculty, and staff. In traditional disaster recovery (DR) planning, a recovery time objective (RTO) is used to determine the requirements for designing and deploying solutions to meet this need. Improvements in the reliability of hardware components have extended mean times between failures, but personnel still must watch for service outages caused by power surges and failures, network outages, and unexpected hardware and software behavior.

The natural progression of improved uptime for services now extends beyond traditional DR to building resiliency into systems from the beginning. Organizational commitment is a critical component, not just for funding the required IT investment to accomplish it but also for creating an organizational culture that includes business continuity planning as part of business practices.

We will consider examples of two critical systems at UMUC: WebTycho, UMUC’s learning management system, and the PeopleSoft ERP, which provides academic self-service functions and back-end HR, finance, and student administration.

Highlights of Changing Ideas of Campus Disaster Recovery

For a long time, higher education’s response to the concept of DR was lip service only. When it was implemented, it was often driven by auditors rather than as a result of institutional commitment. September 11, Hurricane Katrina, SARS, regional blackouts,

and the prospect of numerous other threats have changed all that and have raised awareness of the potential for disasters, consideration for the limits of acceptable risk, and the value of investment to avoid such risks. Security threats have also raised the awareness of risk beyond that of physical events.

Organizations should think of a disaster as any unplanned disruption of service beyond an acceptable period of time. For many organizations—and certainly for higher education—this “acceptable period of time” may be different at different times of the year, or month, or day. Consider how the acceptability for downtime may vary from the start of a semester to final exams or to grade submissions. Despite the variability of this acceptable downtime in the context of a disaster, an organization must plan for the worst-case scenario and set that as the objective for any resilient system.

Traditional DR in the Design of Processes and Technology

Traditional DR strategies emphasize discrete technologies and “bolt on” solutions that typically follow the deployment of technologies and the concomitant development of processes. These strategies are reactive, requiring organizations to speculate on various disaster scenarios and plan accordingly.

With conventional DR models, organizations usually rely on external disaster recovery sites to restore critical systems and processes. Traditional DR strategies also assume that downtime is a given and that RTO is measured in hours or days. Additionally, a significant expenditure of time and effort is required to conduct routine tests and verify traditional DR plans.

In terms of restoration processes, traditional strategies often rely on tape media for the recovery of applications and data. This reliance lengthens the time to service restoration and introduces risk into a successful recovery.

Finally, traditional DR strategies assume that only the most critical applications will be included in the DR plan so that the institution has to recover only a small, manageable, subset of servers. Current multitiered applications require substantially more assets, complexity, and interdependencies to operate, and this complicates the design for DR under the old paradigm.

Resiliency: The New Model of Business Continuity

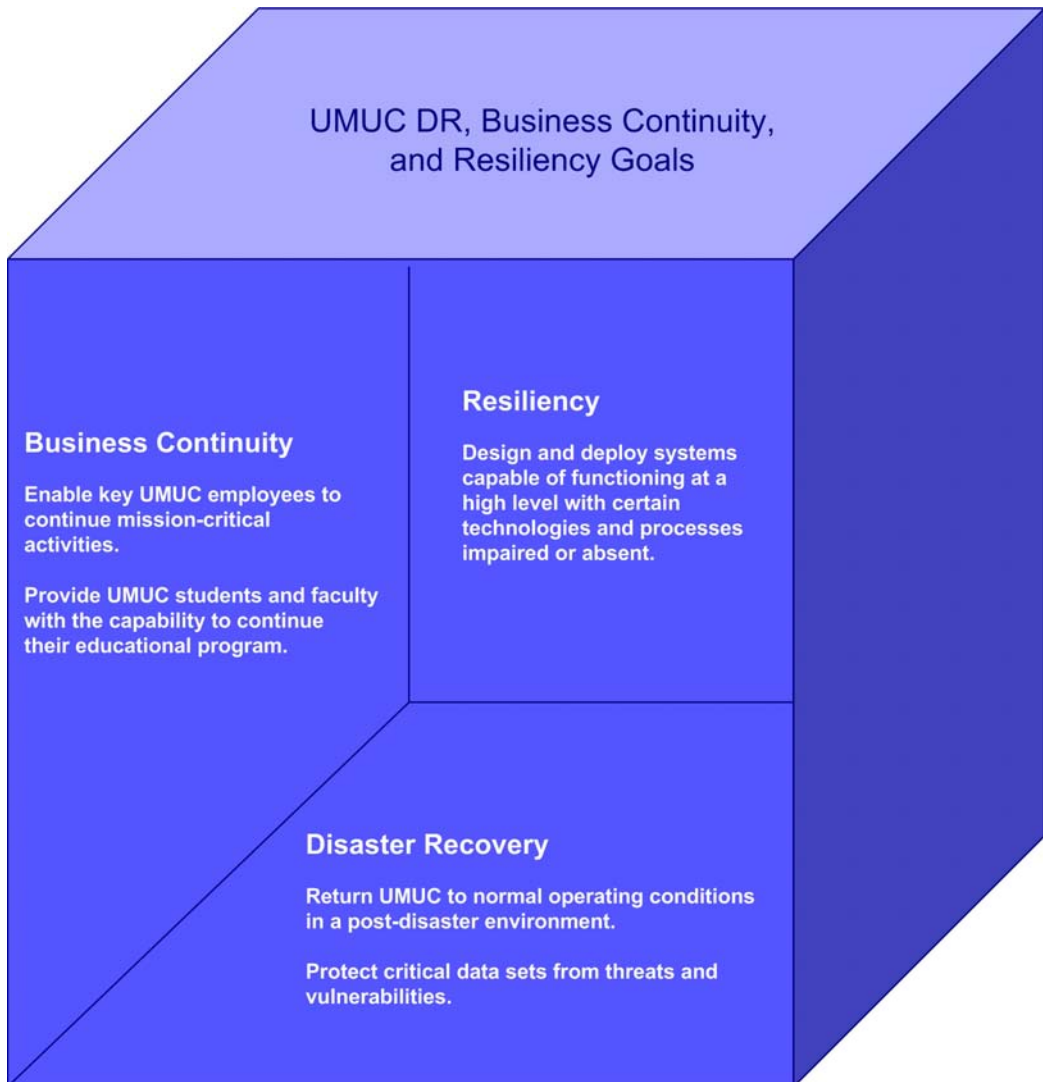
Business continuity refers to an institution’s ability to maintain or restore its business as well as academic services in the event of a disaster. Business continuity encompasses DR, the activities that restore the institution to an acceptable condition after suffering a disaster, but it also includes activities such as assessing risk and business impact, prioritizing business processes, and restoring operations to a “new normal” after an event (Yanosky, 2007). Business continuity is often described in terms of high availability and redundancy in hardware, software, and systems. While business continuity is a more service-based model than DR, it is still largely reactionary. It focuses on building fault tolerances into existing technologies and processes. However, even greater possibilities are revealed in resiliency.

Predicated on considerations at each point of the life cycle, resiliency should be a primary factor of consideration in the analysis, design, and development of all new processes and technologies. Resiliency is thus defined as a mission-critical function of processes and technologies and has an effective “veto” of all solutions that do not adequately provide for it. A staff member representing resiliency should be involved in all strategic and operational discussions when new processes or technologies are considered. Resiliency cannot be omitted based on issues of cost, time, scheduling, internal skills, or other needs. It is as vital as the functions it supports. In short, it must become a core value of the institution for it to succeed.

UMUC Disaster Recovery, Business Continuity, and Resiliency Goals

Figure 1 summarizes UMUC's interdependent goals for DR, business continuity, and resiliency. DR and business continuity are foundational to achieving resiliency.

Figure 1. UMUC DR, Business Continuity, and Resiliency Goals



Examples in the Design of Infrastructure

Taking the approach of building resiliency into the initial scope, design, funding, and implementation of critical IT services requires a foundation that is efficient in both cost and resources. UMUC's goal is to provide a "resiliency blueprint" for new, critical application systems and processes. This will allow a default framework to be used in the consideration of new applications, using a standard set of technologies to provide the infrastructure for resiliency.

The rewards for proactive planning are savings in complexity, maintenance, testing, and cost by leveraging pricing and personnel resources. As the set of mission-critical applications grows, initial investments may appear to be greater, but costs over the life of IT systems will diminish when resiliency factors are built in. Retrofitting established systems is often more challenging and costly than providing the same services via a resiliency framework from the inception.

UMUC's evolution as an institution with its roots in serving the overseas military provides both an uncommon challenge and unique opportunity. At one time the institution operated IT as three distinct, equal divisions, but the momentum to consolidate IT services for efficiency and to use ever-improving global network capabilities allows this resiliency blueprint to be applied worldwide to new application systems.

Using these desired objectives to create a resiliency blueprint, UMUC is adopting the following strategies:

Resilient Design. New mission-critical systems are designed with resiliency in mind. Systems that require the shortest RTO are designed with continual data replication on "hot" (up and running) systems at an alternate data site.

Server Virtualization. Use of emerging server-virtualization technologies such as VMWare (<http://www.vmware.com/>), Xen (<http://www.xensource.com/>), and hypervisor (<http://en.wikipedia.org/wiki/Hypervisor>) allow hardware-independent deployment of applications. Through server virtualization, resources at the primary and secondary sites can be minimized, and a cost-effective model can be adopted to repurpose servers from primary to secondary throughout their life cycle.

Storage Virtualization. Achieving the efficiencies of a leveraged infrastructure for resiliency demands a storage strategy that also includes virtualization, which pools physical storage from multiple network storage devices into what appears (logically) to be a single storage device that can be managed centrally. This reduces time for data backup, recovery, and archiving.

Continual Data Replication. Resiliency requires the transparent, quick recovery of services without the loss of data (or at least as little as the design provides). To achieve this, the notion of transporting tapes to the recovery site is no longer an option. Continual data-replication solutions allow automatic failover to ensure data is made available to secondary systems.

Network Virtualization. To be truly resilient, systems must be accessible with as much transparency as possible when an event occurs to change the background environment (whether through unexpected outage, disaster, or intentional failover for maintenance purposes). Virtualization in the network through numerous technologies including the use of global load balancers ensures that the institution’s customers continue to access systems in the familiar manner they expect.

Multipurpose Use of Standby Systems. The expense, effort, and complexity required to provide resiliency for critical applications through use of secondary standby systems can be leveraged by using this same infrastructure for such things as hosting development platforms and a quality-assurance environment for such things as load-testing or a test bed for “what if” scenarios. Leveraging these systems for multipurpose use can alleviate downtime on the primary production systems.

Building resiliency into systems from the ground up may sometimes influence the choice of specific technologies and packaged IT solutions. By introducing this requirement upfront, it may steer the selection—and certainly the RFP requirements—to ensure that resiliency is built into the research, evaluation, pricing, and selection of solutions.

When building resiliency into systems from the start, an organization must consider the additional complexity itself as a managed risk. Technologies such as synchronous data mirroring, which is recommended for resiliency, can have a negative impact on the availability of primary systems. In certain cases, additional staff resources, more advanced skill sets, heightened technical staff training, and increased time for system testing must be built in and funded as part of the strategy. If they are not, the added protection for “what if” and “in case” scenario testing and failover might compromise primary service availability during normal conditions.

Examples of Resiliency in the Design of Technologies

Tycho. Tycho is the proprietary learning management system for UMUC. The current generation of Tycho, WebTycho, is the product of 12 years of development and was preceded by DOSTycho, WinTycho, and MacTycho. WebTycho provides a mature and stable environment that annually supports more than 150,000 course enrollments worldwide.

In 2005, UMUC began a migration from WebTycho to Tycho Next Generation. This process is predicated on a migration from the current application environment, IBM Lotus Domino, to J2EE. In addition to changing the application environment, the institution will be adding functionality and enhancements to virtually all areas of the system. Unlike previous generations of Tycho that were written to specific operating systems or browser standards, Tycho Next Generation will be accessible from multiple devices.

One key feature of Tycho Next Generation that will add significant resiliency to the system is the Tycho Virtual Learning Management System (VLMS). The Tycho VLMS is an extended client that resides on the user’s computer and reproduces many of the

functions provided by the online classroom through a similar interface. Students can view and respond to messages in class conferences, submit assignments, view reserved readings and other online media, examine the syllabus, and complete other tasks normally requiring a network connection. Upon the next Tycho login, the classrooms on both the client and server will be synchronized and the changes will automatically be made to both classrooms.

The ability to access and interact with classroom content on multiple devices without an Internet connection is a significant step in building resilient technology into a learning management system. In the past, a network connection with constant access to servers has been a requirement of online learning. The VLMS removes the requirements of a ubiquitous Internet connection and of continuous access to the online classroom while working.

Identity Management. With the complex architecture of today's systems, resiliency for one system might require that the same provisions be made for other dependencies. At UMUC, the planned introduction of an identity management system to be integrated into the WebTycho and PeopleSoft student administration system will mean that this new system will be categorized as mission critical.

This initiative will be designed with the same resiliency blueprint mentioned above. Its architecture will be shaped by that model, including the use of virtualization and continual data replication to an alternate site, as well as multitiered redundancy as a default. Previous methodology would have examined DR only after a successful implementation of the primary system, possibly creating a need to rearchitect both primary and secondary systems.

It is UMUC's goal that through the establishment of our own standard design methodologies for resiliency, the effort to design and build resilient systems will become increasingly efficient.

Examples of Resiliency in the Design of Processes

In some instances, the design of resiliency in technology is difficult or not possible. Systems created by external vendors are not subject to the resilient design specifications of the institution. One example at UMUC is the PeopleSoft student administration system.

While we may not have the flexibility in technology design and deployment that is available in homegrown technology, significant resiliency can be added to the process used to deploy the student administrative services. Many elements within this module are process-rich and touched by many hands. As such, they represent vulnerabilities that are potentially as catastrophic to routine business processes as the loss of technology.

One place in which resiliency can be added to student administration relates to the staff that provides these services. Many institutions have experienced personnel choke-

points where the paths of critical processes narrow to a few or even one individual. This can result in constriction of efficiencies or even a termination of student administrative functions if those personnel are unavailable. UMUC is undertaking an extensive knowledge-transfer program that cross-trains staff with similar skill sets and responsibilities and documents roles so that such choke-points are eliminated or minimized.

Another area where resiliency will be added to the student administration business process relates to the location of the activities. Back-office student administration is often tied to a geographic location on campus. Staff interacts with students, their records, and one another via telephones, computers, and protected private networks. UMUC is working to create an extended workspace that can be established at any point in the world. Staff will have the capacity for extended PBX service to phones at their homes or other locations. UMUC is also deploying Hershey Systems Singularity Suite to provide enterprise document management and associated workflow to any properly credentialed desktop worldwide. Finally, UMUC has deployed a virtual private network to provide protected access to the necessary documents and functions at a distance.

Building Resiliency into the Organizational Culture

As SARS and the avian flu have raised the focused attention on pandemic planning, organizational resiliency is often discussed in the context of how the institution will adapt its business procedures and academic delivery in times of disaster or disruption. A complex matrix of variables and assumptions is often used to define actions and outcomes for prescribed scenarios. Most involved in such planning would agree that the precise environment in the event of this type of disaster will be highly fluid and require a plan that can address changes that can occur in days, weeks, or months. This same level of consideration, to enable organizational resiliency, should be applied to disaster recovery and business continuity processes. While testing of these plans is often a neglected component of disaster recovery/business continuity readiness, building consensus for organizational flexibility as part of these plans will increase the institution's chance of success in achieving resiliency.

Like many institutions, UMUC has worked extensively on an avian flu pandemic response plan. That plan is the product of the Pandemic Planning Group, a committee of stakeholders representing the various departments and divisions within the university. The resulting business continuity strategy incorporated input from senior representatives from the provost's office; graduate and undergraduate schools; administration and finance; IT; facilities, planning, and logistics; faculty affairs; legal affairs; and enrollment management. The plan was also vetted by other offices within the institution, including the Executive Committee and the President's Cabinet. Although there were significant difficulties in managing the size, diversity, and competing needs of such a disparate group, the resulting plan reflects both the requirements and complexities most likely to occur in the event of a pandemic.

The plan is constructed around a World Health Organization (WHO) Risk Planning Matrix, which, in turn, is based on the WHO Phase of Pandemic Alert, shown in Figure 2.

Figure 2. World Health Organization Phase of Pandemic Alert*

Inter-pandemic phase New virus in animals, no human cases	Low risk of human cases	1
	Higher risk of human cases	2
Pandemic alert New virus causes human cases	No or very limited human-to-human transmission	3
	Evidence of increased human-to-human transmission	4
	Evidence of significant human-to-human transmission	5
Pandemic	Efficient and sustained human-to-human transmission	6

* Retrieved May 6, 2007, from http://www.who.int/csr/disease/avian_influenza/phase/en/index.html

Within the UMUC plan is a matrix including rows for each of the WHO Pandemic Alert Phases and columns for three functional areas: business continuity, command and control, and hygiene and infection control. The contents of the corresponding cells describe the plans for the required institutional responses. These responses are stated in terms of communications, human resources, academic delivery, student services, IT, and other administrative services. In each instance, the plan identifies the potential threats to national and international university operations and describes the primary goals for each phase.

What It Means to Higher Education

IT in higher education is increasingly transparent. Once novel, the inclusion of course management systems and Web-based resources in face-to-face instruction is now routine. Many students are opting for a complete online learning environment. In their Sloan Consortium report, *Making the Grade: Online Education in the United States, 2006*, Allan and Seaman (2007) observed that there were nearly 3.2 million students in fully online courses. Registrar and bursar services for these courses are available online, and conducting these administrative services on site is the exception, not the rule.

With the increased efficiencies associated with online services come further responsibilities. Universities must take additional measures to ensure that this emerging class of mission-critical academic and administrative system is ubiquitous. With greater reliance on these systems to continue the business of the institution, traditional modes of DR are no longer sufficient. IT professionals need to include resiliency in the design and deployment of the technology to deploy these student services and the business processes that support them. The academic and administrative business of the institution must be supported by resilient systems and processes.

Key Questions to Ask

- What are the critical technologies and processes that need to be resilient?
- To what degree are our current technologies and processes resilient?

- How do we identify techniques and methods to add resiliency to existing technologies and processes?
- What are the most cost-effective ways to add resiliency to existing technologies and processes?
- What are the costs of building resiliency into critical technologies and process? What are the risks of not doing it?
- What are the strategic advantages and disadvantages of building resilient systems in an increasingly online and competitive higher education context?
- What organizational structures are necessary to fully support implementing resiliency in critical technologies and processes?

Where to Learn More

- Camp, J., DeBlois, P. B., & EDUCAUSE Current Issues Committee. (2007). Current issues survey report, 2007. *EDUCAUSE Quarterly*, 30(2). Retrieved May 16, 2007, from <http://www.educause.edu/ir/library/pdf/EQM0723.pdf>
- Federal Emergency Management Agency. (2003). *Building a disaster-resistant university*. Retrieved May 16, 2007, from http://www.fema.gov/pdf/institution/dru_report.pdf
- Glenn, J. (2006). Business continuity v. protecting data: Creating a holistic approach to protect the organization. *Disaster Recovery Journal*, 19(4). Available from <http://www.drj.com/articles/fall06/1904-04p.html>
- Glenn, J. (2006). *One business continuity plan or many minis?* Huddersfeld, West Yorkshire, U.K.: Portal Publishing Ltd. Retrieved May 16, 2007, from <http://www.continuitycentral.com/feature0330.htm>
- Green, K. C. (2006). *Campus Computing 2006: The 17th national survey of computing and information technology in American higher education*. Encino, CA: The Campus Computing Project. Available from <http://www.campuscomputing.net/>
- IT Governance Institute. (2007). *COBIT 4.1*. Rolling Meadows, IL: IT Governance Institute. Available from <http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981>
- Lawson, J. (2005, December 9). A look back at a disaster plan: What went wrong and right. *Chronicle of Higher Education* 52(16), p. B20. Available from <http://chronicle.com/weekly/v52/i16/16b02001.htm>
- Lewis, C. (2007, April 24). *Simple things that could save your institution* (Research Bulletin, Issue 9). Boulder, CO: EDUCAUSE Center for Applied Research. Available from <http://www.educause.edu/ecar/>

- Spicer, D. Z., & Metz, B. A. (2007, March 29). *Post-9/11 emergency response and business continuity changes at Pace University and New York University* (ECAR Case Study 4). Boulder, CO: EDUCAUSE Center for Applied Research. Available from <http://www.educause.edu/ecar/>
- Witty, R. J. (2006, fall). 2005 BCM/DR survey results from Gartner, DRJ. *Disaster Recovery Journal*, 19(4). Available from <http://www.drj.com/articles/fall06/1904-03p.html>
- Yanosky, R. (2007, February 13). *IT recovery time objectives: A survey of higher education practices* (Research Bulletin, Issue 3). Boulder, CO: EDUCAUSE Center for Applied Research. Available from <http://www.educause.edu/ecar/>

References

- Allen, E., & Seaman, J. (2007). *Making the grade: Online education in the United States, 2006*. Needham, MA: Sloan-C. Available from <http://www.sloan-c.org/publications/survey/index.asp>
- Yanosky, R. (2007, March 29.) *Shelter from the storm: IT and business continuity in higher education* (Research Study, Vol. 2). Boulder, CO: EDUCAUSE Center for Applied Research. Available from <http://www.educause.edu/ecar/>

About the Authors

Suresh Balakrishnan (suresh@usmd.edu) is Deputy CIO and Assistant Vice Chancellor at the University System of Maryland. Robert "Rob" Sapp (rsapp@umuc.edu) is Vice President and CIO at the University of Maryland University College. Eric Spangler (espangler@umuc.edu) is Associate Vice President for Information Technology at the University of Maryland University College. Donald Z. Spicer (dspicer@usmd.edu) is ECAR Senior Fellow and Associate Vice Chancellor and CIO at the University System of Maryland.

Copyright 2007 EDUCAUSE and Suresh Balakrishnan, Robert Sapp, Eric Spangler, and Donald Z. Spicer. All rights reserved. This ECAR research bulletin is proprietary and intended for use only by subscribers. Reproduction, or distribution of ECAR research bulletins to those not formally affiliated with the subscribing organization, is strictly prohibited unless prior permission is granted by EDUCAUSE and the authors.