A Report on the Business Continuity Summit
August 2–3, 2006
Part of the 2006 EDUCAUSE Program Plan

Norma Holland, EDUCAUSE Fellow
Cynthia Golden, Vice President, EDUCAUSE

Background
As part of the EDUCAUSE 2006 Program Plan, EDUCAUSE is holding several summits on topics of importance to higher education designed to bring together thought leaders and experts in the community in order to capture the best strategies and behaviors. The Business Continuity Summit, held in August 2006, was attended by about 50 higher education administrators who hold both IT and functional roles. It was led by a professional facilitator who guided the group through a rich discussion of the highest-priority topics.

Definition
“Business continuity” (BC) was defined for the purposes of the summit as the institution’s ability to maintain or restore its business and academic services when some circumstance disrupts normal operations. Business continuity encompasses disaster recovery—the activities that restore the institution to an acceptable condition after suffering a disaster—but also includes activities such as risk and impact assessment, prioritization of business processes, and restoring operations to a “new normal” after an event. The core of the concept is a collaborative and integrated approach in which every department understands and prepares for the role it will play in keeping the whole institution functional in a crisis and viable in the long run.

Speakers
Although the event was focused on discussion, several speakers helped set the stage for the summit. Ron Yanosky, ECAR research fellow, presented preliminary findings from the recent ECAR survey on business continuity. The attendees were surprised at the lack of robust business continuity readiness in higher education today which was reflected in the results. Yanosky stated that most institutions responding to the survey believe their institutions are “at risk,” and that institutional guidance on BC seems underdeveloped at many institutions. Central IT planning is generally ahead of institutional activity, but all BC plan completion rates are low. This is not to say, that institutions lacking completed plans are entirely without response procedures. Even some institutions with no intention of developing BC plans have some documented emergency procedures, and many institutions with “in-progress” plans have built up substantial bodies of individual documented procedures. Plan completion, however, is associated with good behaviors and outcomes, such as greater likelihood of conducting tests and higher overall assessment of preparedness to restore systems. The importance of BC readiness was reflected in respondents’ overall pessimism about business and academic units’ ability to carry out essential operations in the absence of IT systems and services. Among barriers to BC planning, funding stood out: two-thirds of respondents reported they do not have the necessary resources for BC.

Dave Swartz, vice president and CIO at The George Washington University, gave a comprehensive overview of GWU’s BC plan and activities. Because of the campus location near the White House and the events surrounding 9/11, GWU began a university-wide BC program years ahead of many other universities and now has a plan for its disaster recovery program. The plan includes a comprehensive risk assessment as well as a university-wide plan for business continuity. See Dave Swartz’s presentation at http://iss.gwu.edu/cio/index.html.

Tom Richey, Microsoft’s executive director of homeland security, served as moderator for a panel discussion on campus perspectives on BC. The panel was comprised of Wendell Brase, vice chancellor, administration and business services, University of California, Irvine; Catherine Lewis, vice president, technology administration, Xavier University of Louisiana; and Stewart Mixon,
chief operating officer, Medical University of South Carolina. Richey led the panel through a discussion of actual disasters or disruption of services events at their campuses, including hurricanes and earthquakes. Panelists shared their first-hand experiences and offered advice to other campuses. The critical importance of maintaining good communication with staff, students, and the community throughout all phases of a disruptive event was reinforced by all three panelists. Richey made the point that higher education institutions need to be working with the community in a way that can result in an integrated response to an event. Currently, national public systems are not well integrated and responses to disasters can result in duplicate efforts and lack of communication.
DISCUSSION SUMMARY

Business Continuity Viewpoint
It was emphasized by the panel and throughout the summit that BC planning needs to be integrated into our thinking on an ongoing basis—in designing systems and buildings, practicing alternate ways of delivering classes, considering research data, and undertaking normal operations—in essentially in everything we do. Building BC into normal processes results in sustainability for the institution.

Institutional Ownership
Upper administration and boards need to understand the risks of not being prepared, which includes damage to reputations, loss of students, and various costs of being in a reactive mode. Metrics are useful to explain the issues surrounding BC planning. An event, even at another institution, can be leveraged to make the case for BC planning. The remark that “BC is not going to be the main event until it IS the main event” is true more often than not. It is better to spend money on prevention rather than addressing problems after a failure of services. The case for BC readiness needs to be tied to the academic mission, and terminology such as “academic sustainability,” “high availability,” and “resilience” may be better than “business continuity” when having these conversations on campus.

The institution needs to understand that BC is not an IT issue and requires that operational units to take ownership. Upper administration must be supportive; faculty need to be involved regarding instruction and research planning. Senior executives can establish expectations and accountability for departments to ensure their involvement, and IT and auditors (who can also act as compliance drivers) can assist in risk assessment. Upper administration needs to establish governance and leadership on campus for BC, and this entity needs to coordinate with the community and surrounding areas. Expectations of upper administration must be managed, as it is not possible to have systems, services, and facilities up and running quickly.

Promoting the BC plan to the campus can be challenging, but departments are interested in how their systems operate on a daily basis, and their involvement is critical. Enhancements made for the purpose of BC readiness can actually drive overall reliability of daily operations and availability, which can be a big selling point for the institution. Federal regulations with an emphasis on document management (such as Sarbanes-Oxley) can also be drivers and can be useful for many departments on a daily basis as well. Investments that improve recovery can have additional benefits such as aiding in the reduction of maintenance downtime and addressing normal system outages.

Risk Management and Assessment
An assessment of risks is often the place to begin to address BC, and identification of key systems can ensure that those operational units involved have robust plans in place and the funding to accomplish and maintain them. Without risk assessment, there is no good way to understand where the institution stands with regard to BC readiness. Results from risk assessment must be addressed to avoid additional liabilities for the institution.
Plans
The process of planning is as valuable as the plan itself as it encourages continuing attention to the issues; brings awareness to risks; and identifies key players, relationships, and understandings to coordinate a recovery effort. Planning is key and fosters confidence. Training, simulation, and testing of the plan must be ongoing. For example, backups that are seldom tested may not work, which means that data could not be restored in the event of a failure. Lessons learned locally or elsewhere should be incorporated into the plan. A profile describing the institution’s ability to respond and deliver high availability should also be part of the plan.

Operational Strategies
Virtualization of learning (for example, online classrooms) provides more options for BC, and faculty must be engaged to use the online tools on a regular basis. Virtualization of IT infrastructure (flexibility in the logical and physical arrangement of servers, storage, and networks) can complement traditional operations and reduce risk if done well. BC could be an incentive for doing more with virtualization and the establishment of remote data sites to provide redundancy with mirrored data and the use of test machines for fail-over. Reciprocity with other institutions is a consideration here. Distributed servers are a risk because they house critical information and must be addressed in addition to the central IT site. Change management must also be included in BC planning.

Spending and Resources
Funding for BC should be built into the institutional priorities. If, for example, units are taxed across the board to fund BC, then corresponding rebates could be in place for those engaging in good practices. Costs could be spread by working with other institutions to leverage resources as well as by working effectively with vendors prior to an event. BC should be part of every unit’s operational costs, but risk assessment is fundamental to resource allocation for BC. Enhancements and refresh cycles should have built-in costs for BC.

Incident Response
In an actual emergency, safety of people is the first concern, to be followed by recovery of data. Having multiple ways to communicate is critical, and communication was emphasized as vital for the crisis team, employees, students, parents, and the public. Methods that can be employed include automated voice communication systems, alternate Web sites, and a self-registration system to keep track of displaced people and keep everyone informed of the recovery status. In considering the most serious incidents triggering emergency responses on campuses, attendees reported that leadership met daily on the event, campus culture was helpful, staff and vendors were excellent, and departments understood their roles, but there was a lot of emotion involved. IT operations in several cases returned to normal, but the core business and institutional mission was still recovering long after the event.

Next Steps
Those attending the summit described it as a valuable experience where they were able to focus exclusively on this topic in a meaningful way, contribute their thoughts and ideas to the group, and establish relationships with others challenged by the same issues. In early September, Dave Swartz shared his presentation with a wide audience by way of an EDUCAUSE Live! Webcast presentation. In the coming months, EDUCAUSE plans to produce additional articles, executive brochures, presentations at conferences, self-assessment tools, and other resources from the content gathered during the summit.