EDUCAUSE Center for Applied Research

Research Bulletin

Volume 2005, Issue 13

June 21, 2005

Business Continuity Planning:

Process, Impact, and Implications

Bernard Gulachek, University of Minnesota

ECAR

4772 Walnut Street, Suite 206 ◆ Boulder, Colorado 80301-2538 ◆ www.educause.edu/ecar/

Overview

In higher education, increased reliance on enterprise information systems and associated information technologies has raised the expectations for service quality, availability, and reliability. Tens of millions of dollars are invested in systems that promise—and yield—standardized transactions, business process automation, and 24 x 7 service availability. The implied expectation is that systems that offer self-services will be available anywhere, anytime. In light of these heightened expectations, institutions grapple with operational processes and internal organizational relationships to craft service level agreements (SLAs) and varied levels of business continuance in the face of system, equipment, communications, and utility failures as well as potential environmental calamities.

Business continuity planning (BCP) is closely associated with disaster recovery planning (DRP), but BCP covers a broader scope. For purposes of this research bulletin, we shall use the McMillan and Sitko definition of BCP, which focuses on "how to ensure continuity of higher education when we lose access to key people, facilities, information systems, resources, and services."[1] DRP describes processes and procedures for recovering from a natural, man-made, or technology-driven disaster.

While there is no secret recipe or single, easy solution to successful BCP, the topic is certainly part of an overall information security strategy. The International Standards Organization (ISO) devotes section 11 of its 17799 Security Standard to business continuity management. Burton Group's Fred Cohen believes that ISO 17799 "is not the ideal solution to enterprise BCP, in large part because doing what is specified is a lot harder than trying to specify it."[2] What ISO 17799 does well, Cohen said, is to provide guidance for policy development, but

> it provides no useful guidance on the specifics of how often activities should be done, what thresholds should be used for what decisions, the ways these sorts of implementations are handled logistically, the amount of resources needed to carry them out, or any of the other facets of enterprise-scale BCP.[3]

Key ingredients to good BCP include a solid business impact risk analysis and a mix of related plans including information technology (IT) recovery plans, business unit plans, logistics and communication plans, and overall coordination plans. The University of Minnesota (U of M), a large, public, multicampus university system with a highly distributed technology environment, has invested millions of dollars in its information systems, and it has built a business continuity program designed to enable access to those resources and maintain continuity of the enterprise under adverse conditions.

This bulletin describes BCP at the U of M and examines key institutional factors related to it: drivers; decision criteria; planning processes; and critical inter- and intraorganizational relationships, timing, and consultation. The elements of the U of M's operational continuation plans are outlined, the strategies and impact of these plans are discussed, and the implications of BCP for higher education are considered.

Highlights of BCP

In the aftermath of the bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma, on April 19, 1995, the U of M began a close examination of institutional vulnerabilities in terms of the safety of its people, buildings, institutional records, and information systems. The institution launched a comprehensive effort to build a set of operational continuity plans that would reflect processes, policies, and plans to ensure that organizations could continue to function during an emergency or disaster. The goal was to reduce the time that functions would be interrupted and to decrease the time required to return to normal operations. Ultimately, this set of plans would take several years to complete.

Planning Scenarios and Template

Departments were asked to develop plans for responding to each of the following scenarios:

- You cannot occupy your office space, but you can access records and data.
- You cannot access important data, even if you can get into your regular office space.
- You lose a key staff member (due to illness, death, or other causes).

Planning steps were designed to include: creating backup records and files and storing them off-site; giving phone lists to all employees so they can contact each other during business hours, after hours, and on weekends; and designating a “second in command.”

U of M provided a template[4] for departments to use in developing their operational continuity plans. Each plan was to address the following basic elements:

- Identify services, business processes, applications, and normal support tools (business records, computers, telephones, and so forth) that must be sustained during an interruption.
- Ascertain services, processes, or applications that are not critical and may reasonably be suspended during an interruption. Determine how long the unit can function without normal support tools.
- Determine minimal personnel, supplies, data, equipment, and so forth that will be essential to support key functions and recovery efforts.
- Maintain updated contact lists with the names and telephone numbers of key personnel and their recovery responsibilities.
- Identify interfaces to other operating units’ continuity plans. Which units does yours depend on to get its work done? Which units depend on your unit to get their work done?
- Ensure that all personnel with operational continuity responsibilities are trained and prepared to respond during a disaster.

Those departments that were required to submit operational continuity plans[5] could receive support for plan development from the university's Department of Emergency Management.

Reliance on Central Services

In 1995, the notion of enterprise systems was relatively new in higher education. After the mainframe era, institutions developed and implemented many distinct and nonintegrated information systems that were managed unevenly by various schools and departments. These systems ran on a myriad of operating systems, accessed proprietary databases, and were often housed in unsecured physical locations, including under the desks of technology savvy faculty or staff members. The security of the systems depended on the vigilance of the system administrator, and some systems were difficult to keep secure. In the days prior to institutional data warehouses, most systems relied on an internal database that system managers and department heads considered "authoritative." From an institution-wide perspective, each of these systems might have been performing a particular task very well (or not), but the lack of integration between systems and the absence of system management standards was becoming highly problematic. The opportunity to partner with PeopleSoft in the development of an integrated, enterprise-wide student system was considered very appealing from a variety of U of M vantage points.

Along with this development project came a new reliance on central services. U of M made an institutional decision to invest in an enterprise system that would be operated by the Office of Information Technology (OIT) in support of the student services departments. Student services helped define the requirements for the integrated system, and the information technology staff ensured that standards were applied to shared databases, system access and reliability, appropriate user authorization and secure authentication for each application, reliable network connectivity, and, in general, the use of industry-standard system management policies and procedures appropriate to enterprise systems. This new reliance on central technologies brought with it an awesome responsibility for central IT. The terrorist attacks of September 11, 2001, were still five years away when, in early 1996, the Networking and Telecommunication Services (NTS) department began its first planning effort—an operational continuation plan—that was finished in early 1997. A similar planning effort took place for the central IT systems in about 1999.

NTS Operational Continuation Plan

One of the first plans to be developed was the NTS Operational Continuation Plan. In 1995, U of M was deeply involved in a high-profile project with PeopleSoft to collaboratively develop a student information system for higher education. As the impact of the Oklahoma City bombing began to be realized, the institution's vulnerability in terms of the safety and security of human life, property, systems, and connectivity came into high relief. It was deemed that reliance on the development systems was crucial to the continuation of the business of the institution, and, to the degree possible, risk to these assets needed to be mitigated.

The plan was developed under the leadership of the chief information officer (CIO), who championed the idea because he understood that the continuity of business across the institution depended on the networks and systems for which central IT was responsible. The planning effort began in early 1996 and was completed in early 1997. A parallel planning effort focusing on central systems, championed jointly by the provost and CIO, took place in 1999.

Key Drivers for the Plan

Planning efforts for the NTS Operational Continuation Plan were driven by institutional and general higher educational considerations such as

- dependence/reliance on systems to conduct business;
- residence hall needs;
- public service access point/security center (police) needs;
- the emerging awareness of liabilities associated with technology failure (both related to academics/research and fire/life/safety);
- technology drivers including the evolving role of the centralized IT group to manage institutional technologies (for example, the telephone system, campus network, enterprise systems, and PeopleSoft student system);
- maturing technology that required new strategies for security and mitigating risk;
- the recognition that the plan complemented the development of university-wide operational business continuity plans;
- available personnel to create the plan; and
- the emerging realization of liabilities associated with Internet protocol (IP)-based systems such as fire/life/safety (911 systems) and building security/monitoring systems. (At the time, IP was still “best effort,” so a plan was required to demonstrate that everything possible would be done to keep IP-based systems working properly.)

Consultative Planning Process

The planning processes for both the NTS Plan and the Central Computing Plan were highly consultative and included representatives from risk management, emergency services, and police/security, and external vendors such as Qwest.

Internal support services—environmental health and safety, electricians, heating/ventilation/air conditioning personnel, air quality assessment personnel, and university purchasing—were all involved. As a result of this collaborative planning process, all support services departments treat IT as a high priority. This process successfully refined a set of U of M criteria that is used in emergency purchase situations, alleviating potentially long delays due to seeking approval and general processing.

In addition, the plan had executive-level sponsorship—the vice president, provost, and the associate vice president for university operations supported these planning efforts.

BCP's Effect on IT and Departmental Services

Business continuity planning can have a monumental effect on the way the university perceives how it operates, provides services, and conducts critical administrative processes. The planning effort forced certain disciplines to better understand—and plan around—their dependency on IT for their daily operations. Elements such as better planning, good business practices, and increased reliability were a few of the overarching outcomes and positive impacts of BCP at the U of M. Other colleges and universities can also achieve these positive BCP outcomes.

- *Architectural design and new service rollout.* New services and technologies are now designed with failover, redundancy, recovery, risk mitigation, and business continuation as part of the planning effort and development.
- *Operational unit discipline.* Operations engineers are more disciplined in their approach to change management. Greater levels of documentation have resulted from the need for plans that continue services.
- *Customer satisfaction and credibility.* OIT continues to see higher satisfaction ratings for critical services. Additionally, the U of M has seen a migration to centralized services, in part because of the credibility and assurances offered by BCP risk mitigation for these services.
- *Technical cultural changes.* Enterprise-wide services and technologies are expected to include "BCP reliability" as part of the SLAs between OIT and other units of the institution.
- *Resource support for IT BCP.* The importance of IT BCP principles to the institution is underscored by the resource support given. Leaders in both direct and sponsorship roles develop appreciation for BCP discipline while participating in table-top, mock disaster exercises that test the plan's resilience in the face of well-orchestrated, simulated events spanning a myriad of scenarios.
- *Increased communication channels across the institution.* The simple existence of a business continuity plan calls for a well-thought out communications plan. Both technical and administrative components of this plan have created new channels of communication among different constituencies at various institutional levels. These channels have become part of standard operational procedures; they are no longer associated only with a BCP "event."

The BCP efforts have had a long-term, positive impact on the U of M's culture. When IT rolls out a mission-critical application or service today, it automatically architects its systems for redundancy. A similar framework pervades the planning in other U of M operational units and departments.

In the end, it's all about higher-quality service, efficiency, effectiveness, and scalability. When information architects design systems for redundancy, they also design them to scale for capacity. Because mission-critical systems are built with redundancy, operations that require backup or maintenance services can be performed automatically after hours. The old stories of programmers being summoned to the data center at 2:00 a.m. are beginning to fade into history.

What It Means to Higher Education

What are the implications of BCP outside the institution, for higher education in general?

- *Stewardship*—institutions must responsibly manage data, particularly when they participate in publicly funded projects. Although information assurance disciplines can be distinguished among business continuity practices, they are mechanisms designed to protect, preserve, and maintain the usability of data and their systems in the event of a catastrophic failure or crisis.[6] The Gramm-Leach-Bliley Act (GLBA), the Family Educational Rights and Privacy Act (FERPA), the Visa Cardholder Information Security Program (CISP) standards, and other compliance-related accountability measures set the bar for all institutions of higher education. Research institutions carry the additional responsibility of producing research data as part of grant requirements. To what extent are institutions of higher education responsible for data loss or violations that could have been mitigated or avoided with a proper business continuity plan? Are the liabilities greater with—or without—the plan? These questions become increasingly important, as accountability for compromised data can lead to financial penalties, litigation, and loss of credibility.

- *Management*—disciplined technology management methodologies and approaches are now essential in an enterprise environment. How disciplined are technology management processes in today's higher education institutions? Are change management processes in place—and followed—when critical servers or network components are either swapped or upgraded to new operating system revisions? Is the same process in place when newly developed code appears ready for production? Is there a well-understood and communicated rollback plan in the event of an unforeseen circumstance that will ensure a safe fallback strategy if indeed needed? Almost 70 percent of the U of M's technology resources are distributed, but they provide local system support. Predictable approaches and outcomes to enterprise and local technology management are essential for BCP success. Will higher education insist on this discipline for the management of its critical services?

- *Innovation*—technology development and management must be flexible enough to accommodate innovation. Can academic and scientific inquiry, "tinkering," and research exploration occur in the context of disciplined technology development, and is a reliable production environment in place for system management? During the process of BCP, the U of M discovered that unbridled development can occur as long as developers keep in mind mechanisms that ensure reliability and redundancies—two elements of successful BCP practices—when they build IT systems and services. New innovations must pass the threshold of business continuity requirements prior to introducing a service in a production environment.

- *Costs*—consortium buying presents opportunities to reduce costs. Higher education has experienced excruciating financial strain over the past several years. The U of M, for instance, has seen a 12–15 percent increase in tuition over the previous two years amid continually declining state support. BCP addresses both the need to control costs and protect investments in the face of budgetary challenges. Prudent planning and aggregated/consortium buying can help mitigate hardware and software expenses.

- *Collaboration*—opportunities for interinstitutional resource sharing result from leveraging existing assets, human capital, and linkages between institutions. Strategic opportunities may exist in the form of interinstitutional collaborations that enable institutions to leverage their core competencies, skill sets, and resources. By leveraging the interconnectivity that exists between institutions and other interoperable technologies, creative partnerships can be forged to position institutions as hot or cold business continuity/disaster recovery backup sites for each other; the U of M has been testing its storage area network (SAN) technology with another institution to investigate this as an innovative approach to creating alternative hot or cold sites. By recognizing the importance of business continuity—and by thinking strategically about the effective use of assets—higher education can apply collaboration to architecting redundancies, providing backup, and sharing storage across institutions.

Key Questions to Ask

- How can our institution determine its readiness for BCP and the associated discipline/diligence needed to maintain the plan?

- What are the most important considerations when prioritizing services and their corresponding continuity measures?

- How can our institution determine a BCP model that best fits our environment and organizational culture?

- To what degree should distributed technology services be incorporated into the institution-wide business continuity plan?

- What criteria should be used to define the technologies that should be included in the plan?

- How can our institution leverage BCP to encourage alignment and simplify the complex technical environment?

Where to Learn More

- Continuity Central, a source for articles, checklists, principles, and sample business continuity plans, <http://www.continuitycentral.com/bcpd.htm>.
- A. McCord and G. Thiele, “Campus-Wide Planning for Business Continuity and Emergency Operations,” presentation at the 2000 EDUCAUSE Annual Conference, Nashville, Tennessee, October 2000, <http://www.educause.edu/ir/library/pdf/CSD1683.pdf>.
- State of Arizona, “Business Continuity/Disaster Recovery Plan (BCDR),” October 15, 2001, <http://gita.state.az.us/policies_standards/html/p800_s865_bcdr.htm>.

Endnotes

1. M. A. McMillan and T. D. Sitko, “Managing University Business Continuity,” in P. A. McClure, ed., *Organizing and Managing Information Resources on Your Campus* (San Francisco: Jossey-Bass, 2003), pp. 113, <http://www.educause.edu/ir/library/pdf/pub7007j.pdf>.
2. F. Cohen, “Business Continuity Planning for IT,” Burton Group, March 24, 2005, pp. 17, <http://www.burtongroup.com/Content/doc.aspx?cid=632>.
3. Ibid.
4. University of Minnesota Operational Continuity Plan template, <http://www1.umn.edu/prepared/pdf/cont_plan_temp.pdf>.
5. The following 16 U of M units are required to complete full operational continuity plans to ensure work resumes as quickly as possible in the event of an emergency: Office of Budget and Finance; Building Codes; Bursar Office; Central Computing Operations; Emergency Management; Environmental Health and Safety; Facilities Management; Office of General Counsel; Housing and Residential Life; Human Resources (Employee Benefits); Human Resources (Employee Relations and Compensation); Networking and Telecommunications; Office of the Registrar; Research Animal Resources; Research Subject Protection; and the University of Minnesota Police Department.
6. J.-N. Ezingeard, E. McFadzean, and D. Birchall, “A Model of Information Assurance Benefits,” *Information Systems Management Journal*, Spring 2005, pp. 20–29.

About the Author

Bernard Gulachek (bernard@umn.edu) is Director, Office of Information Technology, at the University of Minnesota.

Copyright 2005 EDUCAUSE and Bernard Gulachek. 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 author.