Chapter 8
Managing University Business Continuity
Marilyn Ayres McMillan and Toby D. Sitko

Organizing and Managing Information Resources on Your Campus
Polley Ann McClure, Editor

A Publication of EDUCAUSE
Simply introducing the term *business continuity* into the vocabulary of higher education leaders and trustees indicates the incursion of information technology (IT) into university and college life. Automated information systems and the technologies that support them are among the institution’s most precious—and most vulnerable—assets. Our institutions have become increasingly dependent on IT in the areas of student life, learning, and administration. How to ensure continuity of higher education when we lose access to key people, facilities, information systems, resources, and services is the essence of business continuity planning.

Many information systems hold irreplaceable intellectual property and data. They depend on formal and informal relationships among people to keep them current, and they rely on miles of complex infrastructure that can be compromised by natural incidents and human error, up to and including full-fledged disasters. Although it can be difficult to quantify the true cost of information systems, they certainly represent major institutional investments.

Our thanks to Margaret F. Plympton of Lehigh University for her insightful, constructive comments on an early draft of this chapter. We are also grateful for the tremendous efforts of all of our New York University colleagues, both before and after the terrorist attacks of September 11, 2001, when we all learned new lessons in business continuity management.
To mitigate the risks of losing access to the systems, we must determine which processes are critical during and immediately following a crisis and how quickly each of those processes must be restored.

Challenges for Managing Information Resources

Creating, managing, and preserving intellectual property and institutional records have been the purview of higher education for centuries, but responsibly managing electronic information resources is a relatively new science and art. Technology costs and the rapid pace of technology change do not easily fit into established budget structures. Policies that govern access to licensed, confidential, or proprietary documents must be revisited in the light of on-line systems. Structures and practices that ensure the continuity of business in the physical world are necessary but insufficient to ensure the same continuity when critical institutional assets are on-line. As a result, institutions must rethink their recovery assumptions.

Institutional business involves complex dependencies that must be managed across the organization. Whereas the chief information officer might be responsible for the integrity and reliability of the campus network, the stewards of the data and information that comprise institutional memory reside in departments across campus. Effective business management involves a broad network of individuals, processes, and systems in both the physical and electronic worlds. Sound approaches to continuity planning serve to protect institutional assets, control exposures and risks, and enable proactive management of service interruptions.

Electronic information systems that drive institutional business proliferate not only in central data centers but also throughout colleges, schools, and departments. To manage their budgets or personnel data, deans and department heads may depend on local shadow systems that provide tailored reports. To create and protect their intellectual property, faculty members may store files without
applying the best physical and data security practices. Because these institutional assets are scattered across campus computers, managing and protecting them requires broadly coordinated efforts.

The past decade has seen a rapid convergence of previously discrete technologies that support higher education. Although significant differences still exist between how large administrative systems and smaller systems are built and managed, the bright lines that once separated those technologies have begun to blur. Perhaps most significant, the faculty, students, and staff of institutions are likely to use a spectrum of technologies in their daily work. As a result of this ongoing convergence, some campuses see the need to continually change the organizational structures that support information resources. The drivers for these organizational changes can be rooted as much in institutional culture as in technology.

One manifestation of organizational change is the migration of responsibilities between an institution’s central IT unit and IT units located in schools and departments. When technologies are not interdependent, local or departmental support for IT allows departments to tailor the IT environments with specialized software applications and locally managed help services that serve departmental needs. With the emergence of newer systems that rely on centralized authentication and authorization services fed from institutional directories, some responsibilities are swinging back to central IT. Managing the continuity of institutional business in this ever-changing environment requires creative leadership and cross-organizational cooperation.

**Risk Awareness**

New York University is keenly aware of risk, with its main campus located approximately one and a half miles north of the World Trade Center site. The impact of the September 11, 2001, terrorist attack on the World Trade Center was enormous on every imaginable front.
This event, as well as other major incidents, highlights the need to be aware of how different risks affect the spectrum of student life, instruction, research, administration, physical plant, campus utilities, public safety, and public and government relations. What would result from the partial or complete destruction of key buildings and the records they contain? What if the systems that control fire alarms and security systems in residence halls, classroom buildings, or administrative facilities are compromised? How can an institution manage incidents in ways that minimize risks to future enrollment, alumni support, and overall viability? What if campus facilities and systems are functioning, but no one can access them because of environmental pollutants or unsafe conditions? How does an institution operate in the face of long-term inaccessibility to communication infrastructure? Who has the authority to declare a campus emergency, and where are emergency protocols maintained? Where do officials meet when the usual places are no longer available? How does an institution determine how much risk is acceptable? What will insurance providers require in terms of well-articulated, annually reviewed plans? How involved is campus risk management in business continuity planning? To what degree are community and campus emergency plans linked to campus continuity plans? How can the institution serve its community in responding to community-wide or citywide emergencies?

For business continuity to work, many people must be involved. Trustees will want to ensure that the institution has an executable plan. In large measure, the most successful plans will be those constructed with the full support of the trustees and the campus community. Senior officers and academic leaders ensure that plans are developed, tested, and kept current. Typically, the chief operating officer of each business and academic unit will be responsible for the unit plan. Because they will be part of the plan execution, senior officers must articulate clear lines of authority for situations that disrupt normal operations. A continuity plan should designate who
will manage the initial crisis and who will be part of the incident management team.

**Emergency Preparedness: Wise Investments, Rational Structures, and Good Practices**

Awareness that once unimaginable incidents can disrupt university life has motivated leaders to place renewed emphasis on emergency preparedness. Successful preparedness is, as posters proclaimed for decades, no accident. Everyone affected must be ready to do the right things in the right ways, typically over an extended period of time, as an incident unfolds.

With increasing reliance on IT, not only at institutions but also in the wider world, staying prepared to handle emergencies puts IT in a more intense spotlight than ever before. Even institutions with long and successful histories of responding effectively to emergencies must develop their proved strategies to incorporate emerging uses of technology in daily institutional life and in emergencies, as well as the typically distributed management responsibilities for what may become crucial resources.

The right things to do, highlighted in much management literature, can be itemized in a logical sequence. One step need not be fully completed before another begins. Ensuring the continuity of institutional business refers to a coordinated strategy for managing a recurring cycle:

- Risk assessment
- Continuity planning
- Continuity readiness
- Incident management
- Restoration to the new normal
- Perpetuating the cycle
Risk Assessment

Identifying essential IT systems and services, classifying their criticality, and estimating their viability in an outage is the foundation. The IT systems and services to consider are the ones the institution runs centrally, the ones run by other offices at the institution for themselves and sometimes for others, and services acquired from outside providers. With the evolving reliance on IT for new functions, such as instructional technologies, and in new places, such as managing building heating, ventilation, and air conditioning systems and access control systems over the network, more resources than ever before must be considered and more participants than ever before must be included in the practice.

Three eventualities are useful to consider in estimating how long an outage an institution can sustain:

- What if the system or service—telephones, networks, Web site, e-mail, application, local or central computer—goes down, but people can stay in or get to offices, residences, or facilities?
- What if the system or service is running, but people cannot stay in or get to sites?
- What if sites, systems, and services are unavailable?

Incorporate time in your thinking. Consider peak and other critical times for a system or service, prime-time needs and off-hours expectations, and requirements of the academic calendar and business cycles.

A classification scheme helps communicate priorities. Some systems and services fall readily into the category “must have available around the clock, all year, especially during an emergency.” Others naturally have a much lower priority: “Get back and running whenever things get back to normal, up to thirty days or more after the
“outage.” Establishing the midrange categories can be problematic because it may be difficult to reach agreement about the priority for some systems and services. Requiring a documented business continuity plan for every highest-priority system and service, as well as periodic participation in continuity readiness activities, can influence the classification decision.

A straightforward risk assessment template facilitates the assessment for each resource and enables aggregation of the information across the spectrum of services and participants. Typically, universities are experienced at such practices for administrative applications. Now may be the time not only to refresh your thinking about those systems, but also to extend your assessment to include the outage risks associated with IT resources supporting all the other elements of university life.

Continuity Planning

Opportunities to improve and perhaps overhaul business continuity management plans will surface in virtually any risk assessment activity, whether it is an institution-wide or department-based activity. Continuity planning activities focus on determining four separate but related courses of action:

- How to conduct business in the event of an outage of systems and services
- What steps to take to prolong the availability of key systems and services in an outage
- What information and training to provide managers, staff, and vendors who will be involved
- What awareness activities and other preparations to provide for the university community

Models developed for managing continuity in the corporate world can be useful, but are only part of the story for universities,
especially for those with students in residence, numerous facilities, or substantial public constituencies. It can be useful instead to consider models used by municipalities.

Continuity planning is by its nature iterative and collaborative. Continuity plans for central services influence departmental planning. Continuity needs of departments may drive changes in central service plans. Opportunities to leverage resources are possible. So are possibilities for gaps and misunderstandings. The most inhibiting factor is that continuity planning is usually everyone’s fourth priority, on plates already too full. Although it is essential to focus planning activities on the highest-priority elements, it is important and appropriate to encourage broad-based individual and department efforts to get better prepared.

Planning forces an institution to reach a balance between acceptable risk and acceptable one-time and recurring costs. Business continuity planning includes the following steps:

- Building awareness
- Analyzing business functions to assess operational, academic, fiscal, legal, or regulatory risks
- Determining the recovery time frame for each business function
- Identifying recovery alternatives within specified recovery time frames
- Creating, testing, revising, and updating plans
- Revising job descriptions to include continuity planning

**Continuity Readiness**

Readiness involves executing the elements of continuity plans that prepare people to respond to a disruption. Some elements of readi-
ness must become routine components of everyday activities for many people: refreshing emergency contact lists, running backups, and refreshing batteries in safety kits, to name a few. Some readiness efforts are periodic, such as verifying the recoverability of backups and running a training session for new staff. Others may be one-time large- or small-scale projects for particular units. Central IT staff might add alternate electric power sources for a computing facility. A student services office might relocate or digitize its collection of paper. An associate dean may work with faculty and instructional staff to establish phone trees.

Still other readiness activities entail broader coordination to exercise key elements of the continuity plan. It is not enough, for example, to have alternate sites for system and service operations or for coordination of university emergency management activities. Managers and staff must ensure that the systems and services can be made operational in the sites and readily used at designated locations.

The important tenet here is that continuity readiness is an ongoing responsibility of every senior officer and direct reports and many staff. The time needed to pay attention to this critical function must be factored into individual and group work plans. The ability to pinch-hit in an emergency must be in everyone’s skill set. Willingness to collaborate on readiness activities across institutional borders must become an integral component of university citizenship. Capacity to promote this attention, skill, and willingness is a critical success factor for the chief information officer and the chief executive.

Incident Management

Incidents come in all sizes and at any time of day and night. Most institutions have well-exercised procedures for handling emergencies of contained scope and scale. As those procedures have come to rely on IT resources, both local and central, it is important to incorporate their viability as part of risk assessment, continuity planning, and continuity readiness efforts.
Transition of an incident from contained or transient to broad and enduring may or may not be obvious to beholders. It is highly desirable to have developed, as part of continuity planning, a protocol for handling this transition: who will declare the extent of emergency response required; who will be notified; and where, if needed, emergency response centers will be located. Determining centers and participants as part of the continuity plan and maintaining components as part of readiness activities enables everyone to avoid ineffective scrambling when the time comes to mobilize.

In managing our institutions in normal times, we follow protocols of deliberative consultation, as well as various combinations of orchestrated and individual or unit actions. Depending on the nature of the emergency, a similar approach applies to incident management, but with some key differences:

- Time frames for decision making are accelerated.
- The pattern of which actions are orchestrated and which are unit or individual may change.
- Public relations about the institution’s handling of the situation may be heightened in all media.
- New developments may or may not radically alter the situation at any time.

This suggests adopting an “accordion” approach in the emergency response center: personnel come together regularly for coordination and then disperse for action in departmental units or as cross-functional teams. Select with care those who need to be in the centers, and conduct departmental gatherings and activities elsewhere. Designate methods and times to reconvene and maintain contact.

At New York University, the primary emergency response center is operated by Protection Services, under the leadership of the chief of campus security. Telephone, radio, network, and computer
services at the center are supported by Information Technology Services (ITS). The center includes small offices for representatives of units active around the clock in handling the response, such as ITS, Buildings Maintenance and Operations, Student Housing, and Public Relations, as well as a larger meeting room. In non-emergency times, the center serves a completely different purpose. When warranted, at another location, NYU transforms the ITS Client Services Center and Telephone Switchboard into an emergency call center, staffed around the clock and augmented with volunteers, to assist students, faculty, and staff affected by an emergency.

The work of the chief information officer in the management of the large-scale incident is complex:

- Collaborate with other senior officers to manage the overall response
- Guide IT management in running the IT continuity activities
- Lead others in whatever other systems, services, and problem-solving activities may be required
- Reserve some personal and organizational capacity for addressing the next surprise
- Attend to the human impact of the crisis on oneself, managers, staff, and colleagues

In addition to their planned efforts to support the emergency response center and keep systems and services running, IT staff may be called on to perform any number of previously unplanned activities during the emergency. Some examples include producing data in various configurations, coordinating call center volunteers from many offices, equipping new venues for relocated activities, and acquiring and distributing inventories of special gear. In a broad-based emergency, those staff may also be experiencing personal impacts from the
situation, such as problematic transportation to and from work or worries about the safety of loved ones. Consider ways to acknowledge and ease the toll on them, while respecting their privacy.

**Restoration to the New Normal**

Although the demarcation between the end of an emergency situation and the start of routine operations is often not clearly delineated, it is important to declare the end at a time of the leadership’s choosing. Close the emergency response center. Return call center availability to normal hours. Reduce the frequency of emergency coordination meetings. Get some sleep. Appreciate and recognize the participants.

Do not expect things to get back to familiar normal patterns anytime soon. If nothing else, everyone’s conception of what is normal now includes a new eventuality that actually occurred, along with everything they learned in that experience. Even more important, leaders, managers, and staff may be exhausted and need time to recover, a rhythm that will vary for each individual. Nevertheless, demands of everyday activities will manifest themselves, with expectations for familiar service levels and response times. Those demands may indeed be heightened in the aftermath. If the institution is concerned about whether current enrollments, future applications, or donor and sponsor support will be adversely affected by news of the emergency, you may choose to work particularly hard immediately to avoid downturns. Such initiatives may well engage many of the service providers now in recovery. At the same time, the various units, IT among them, must assess the impact of the recent experience in the following two dimensions and revise their work plans accordingly.

- What delay, if any, did the emergency inflict on targets for projects in progress?
- What lessons learned from the emergency can be factored into those projects and life in general?
Anticipate that the interest in and tolerance for risk assessment and continuity planning will fall amazingly rapidly on everyone’s agendas, even those of the zealots. Make every effort to capture expeditiously the reflections on lessons learned and turn them into visible improvements for the next time—because there will be one.

**Perpetuating the Cycle**

Changing conditions at the institution, among continuity service providers, and in the wider world dictate that institutions undertake regular efforts to keep their business continuity management plans vital. This can be accomplished at several levels; for example, institutions can

- Publicize reminders of existing plans for the general community at least once during each academic cycle
- Schedule continuity preparedness drills at least once a year
- Establish a process to incorporate new systems, services, and functions in the university plan
- Revisit and refresh departmental and university continuity plans at least annually
- Encourage participation in professional seminars on risk assessment and business continuity
- Develop a regular practice to formally review the risk assessment and plans with senior officers

Chief information officers can be catalysts in promoting continued attention to business continuity, both within the IT functions and throughout the university. Chief executives and other senior officers set the tone that business continuity is not simply the job of technologists; it is a university-wide priority.
The Right Level of Investment

A salient responsibility for senior officers and trustees is determining the right level of capital and operating investment in business continuity management. Arriving at the right answer for an institution can be complicated. Even the Federal Emergency Management Authority, with cadres of experts engaged, is struggling to modernize its cost-benefit calculation models to assess return on investments in disaster prevention projects proposed by nonprofit organizations for funding, as part of its emergency mitigation program. Some rules of thumb may be helpful:

- Risk management is the starting point. What is at risk at your institution in the event of a substantial IT outage? What is your institution’s general approach with regard to investing in risk avoidance?
- Prior and current spending levels for business continuity management are a second consideration. Are you getting full value for your dollar, given your latest risk assessment? Can you leverage better coverage from current levels?
- Balancing your IT investment portfolio is another element of the decision of how much to spend in both dollars and staff effort. Although business continuity management is necessary, it likely is not the only IT investment sufficient to meet your strategic institutional needs. A new Web site that might be down for a few hours someday may be preferable to deferring all Web presence until off-site backups are arranged for existing systems—or maybe not. Prioritize and pace investments effectively among your IT needs.
- Building business continuity management costs into the project and operating costs of prospective new systems and services is ultimately the way to perpetuate the cycle. Evaluating the cost-effectiveness of proposed new initiatives should incorporate the incremental costs of business continuity measures—appropriate to the identified continuity classification—in calculating the total cost
of acquisition and ownership. Publishing a template of business continuity considerations for project proposals can be useful.

Conclusion

The right way to do these business continuity activities boils down to the people in the IT organization and, for that matter, throughout the institution and their readiness to be service-oriented and innovative team builders, problem solvers, communicators, and results producers and to be resilient under pressure.

Everything you do to make the IT organization more effective in today's environment positions managers and staff in IT, and throughout the university, to be more effective at business continuity management. Applying ideas articulated throughout this book can make the difference.

Successful business continuity management is crucial. It enables people and institutions to be as prepared as they can be to respond to unexpected disruptions. In serious circumstances, it may protect the health and safety of members of the university community. In extreme cases, it can enable the institution to remain viable, retain students and attract prospects, and sustain the confidence of sponsors and donors for the future. This keeps business continuity management high on the list of concerns of university leaders and trustees. Addressing their concerns requires that the chief executive and the chief information officer exercise the familiar leadership virtues of vision, encouragement, and persistence in this domain.