

Roadmap

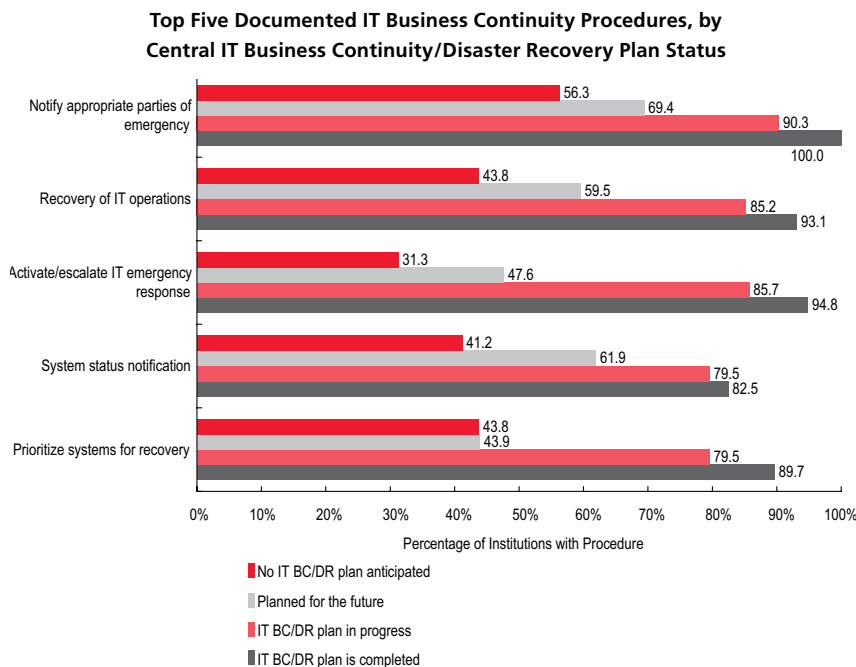
TOOLS FOR NAVIGATING COMPLEX DECISIONS

Shelter from the Storm: IT and Business Continuity in Higher Education

By Judith A. Pirani and Ronald Yanosky, Fellows, EDUCAUSE Center for Applied Research

KEY FINDINGS

- ▶ About half of respondent institutions reported disruptions in the past five years that triggered information technology (IT) emergency responses.
- ▶ Top drivers of business continuity (BC) planning are business best practice, audit requirements, and awareness of recent global disasters. Top barriers are lack of adequate funding and failure of business and academic units to define business continuity needs.
- ▶ Though almost all respondents reported at least some documented business continuity–related procedures, completed formal business continuity plans were much less common than plans in progress or anticipated. As the figure illustrates, institutions with completed formal IT business continuity/disaster recovery plans were more likely to report specific documented procedures than those lacking them.
- ▶ Chief business officers (CBOs) are generally more positive about business continuity readiness than CIOs, though not radically so.



One may associate business continuity planning with extraordinary events like a hurricane or an earthquake, but challenging, disruptive events happen at higher education institutions with surprising frequency. A commonplace event, such as an electrical outage or an equipment failure, can potentially immobilize day-to-day activities. The EDUCAUSE Center for Applied Research (ECAR) study, *Shelter from the Storm: IT and Business Continuity in Higher Education*, makes it clear just how often such episodes occur; about half of the institutions surveyed reported experiencing disruptions in the past five years that triggered IT emergency

This ECAR Roadmap synthesizes 340 responses to a May 2006 survey of EDUCAUSE member institutions, 247 responses to a separate, shorter October 2006 survey of National Association of College and University Business Officers (NACUBO) member institutions, and interviews with executives and IT staff members involved in business continuity. For the full analysis, see the 2007 ECAR study, Shelter from the Storm: IT and Business Continuity in Higher Education, by Ronald Yanosky. To order the full study or to learn about subscribing to ECAR, visit the ECAR Web site at <http://www.educause.edu/ecar/> or contact us at ecar@educause.edu.

TERMINOLOGY

Traditionally, IT units have used the term *disaster recovery* to refer to their disruption planning and response activities, which mainly focus on achieving rapid technical recovery through data and system restoration. In light of the growing interdependence of technology, business, and academic services, however, and following a trend evident in disaster preparedness standards and professional certification, ECAR sees disaster recovery as part of a more inclusive paradigm: business continuity.

This ECAR study defines *business continuity* as the institution's ability to maintain or restore its business and academic services when some circumstance threatens or 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 assessing risk and business impact, prioritization of business processes, and restoring operations to a "new normal" after an event.

responses. Seventy to eighty percent of institutions going through disruptions reported the kinds of consequences that bring campus work to a halt: networks down, business and academic applications unavailable, communications systems not functioning. For a college or university, responding effectively to such circumstances can be the difference between a modest interruption and a severe blow to the institution's viability, providing a powerful financial incentive to optimize its business continuity readiness.

Business continuity is truly an institutional activity. IT must play an integral part, as IT's role in academic and business operations has grown enormously in the past decade. At the same time, business continuity's holistic nature means that IT cannot "own" it or deliver it single-handedly. The business continuity paradigm reaches beyond technical recovery to consider the institution's overall academic and business functioning as the test of a successful emergency response. Consequently, *Shelter from the Storm: IT and Business Continuity in Higher Education* looks at many aspects of IT support for business continuity, including institutional context, business continuity planning activities, supporting infrastructure and technologies, awareness and testing programs, disruptive incidents experienced and assessments of response, and finally—to get an alternate campus viewpoint—the views of institutional business officers on some of these items.

Among our respondent institutions, business continuity planning was a work in progress. They clearly see it as an important activity worth the expenditure of considerable resources. Nevertheless, IT support for business continuity often looks like a background process, attended to as resources and contingencies permit, rather than a focused, high-priority activity. Virtually all respondents reported having some documented business continuity-related procedures, but relatively few said

they had completed major business continuity planning documents. Reports of planned activity indicate that many institutions hope to make up such deficits, but, because most respondents disagree that they have the necessary funding to deliver IT support for business continuity, it will likely be a struggle for many to find the resources to realize their ambitions. Yet the benefits are apparent for those institutions that tackle business continuity readiness aggressively, for we found that institutions engaged in recommended business continuity best practices tended to report better outcomes.

Institutional Context: High Support, Lower Action

CIO survey respondents on the whole agreed that awareness of the need for business continuity planning was high at their institutions. On our scale from 1 (strongly disagree) to 5 (strongly agree), mean agreement was 3.59, and a total of 61 percent agreed or strongly agreed that awareness was high. Nonetheless, respondents don't seem to think that greater business continuity awareness has been translated into broad institutional action or funding. They tended to agree that senior management placed high priority on business continuity planning, but when asked whether business continuity was one of the top-three IT issues at their institutions, they averaged an unenthusiastic 2.92 response. Asked their level of agreement that central IT is actively involved in business continuity planning conducted by other units, respondents averaged only a neutral response (3.09) regarding involvement with business units. They also disagreed overall that business continuity principles were woven into institutional business operations. Nearly seven in 10 CIO survey respondents disagreed or strongly disagreed that their institution had the necessary funding to deliver IT support for business continuity.

METHODOLOGY

- ▶ A literature review from journalistic, academic, and IT practitioner sources, as well as business continuity–related standards and frameworks
- ▶ Invitations sent in May 2006 to 1,615 EDUCAUSE member institutions, generating 340 responses to the Web-based survey
- ▶ A shorter companion online survey in October 2006 of NACUBO membership, which generated 247 responses—including 52 institutional matches with the IT administrators’ survey (responses to both surveys from the same institution)
- ▶ Fifteen interviews with individuals involved in business continuity concerns, including higher education CIOs and chief financial officers, conducted at a two-day EDUCAUSE executive summit

Fostering a Virtuous Cycle of Benefits

There is a widespread tendency to equate business continuity readiness with having some sort of formal plan, and the survey results seem to show that working on business continuity plans situates respondent institutions in a virtuous cycle of benefits—though whether plans drive good actions or vice versa is harder to say. We asked about three different kinds of business continuity planning documents: **institutional risk assessments**, which identify the threats an institution faces, assess their potential impact, and prioritize the associated risks; **institutional business continuity plans**, recommended in some business continuity standards as an overall guiding document that departmental plans align with; and **central IT business continuity and disaster recovery plans**, which deal with IT’s response to disruptions. Between 9 and 17 percent told us their institutions had completed these activities. Those who said work was in progress made up the largest response group in each case.

But an incomplete plan does not necessarily mean the absence of documented business continuity procedures. In addition to asking about formal planning documents, we asked about documented component procedures that are typically contained in plans but which may also exist as stand-alone procedures. Such procedures were much more common than the institutional risk assessment/plan completion figures imply. For example, among 13 different central IT procedures related to business continuity that we asked about, the median number of documented procedures was eight. Institutions with plans in progress averaged almost as many documented procedures as those with completed plans. Thus, institutions lacking a completed plan may nonetheless have substantial documentary coverage at a procedural level.

This is not to say that completing business continuity plans has no benefits. Factors such as agreement that business continuity–related procedures are kept up to

date, conducting business continuity tests, and possession of operational alternate IT sites all tended toward better measures among those with more advanced institutional risk assessment and IT business continuity/disaster recovery plan status.

A Healthy Mix of Backup Methods, but Awareness and Testing Need Work

Virtually all respondents reported widespread use of backup to vault-stored media, and this was fortified at over half of respondent institutions by at least selective use of data-mirroring and high-availability techniques. A more worrisome situation exists regarding alternate IT sites that can be used when primary sites are unavailable. About three in ten respondent institutions reported having an operational alternate site, but only half of these were located more than five miles from primary campus IT operations.

Business continuity awareness and testing were among the areas of greatest weakness in the overall business continuity readiness profiles of our respondent institutions. Nearly eight in 10 CIO survey respondents disagreed or strongly disagreed that their institutions regularly communicate business continuity awareness issues. Only about 35 percent reported conducting tests of IT readiness to support business continuity, and some of these said they carried out tests less than once per year. But testing institutions are positive about the usefulness of tests: seven of 10 agreed or strongly agreed that they had used test results to improve business continuity plans and procedures.

Incident Experience, Response, and Performance

When asked how they would assess aspects of their institution’s response to the most serious disruption they had experienced in the past five years, respondents were

RECOMMENDATIONS

Based on its findings in *Shelter from the Storm: IT and Business Continuity in Higher Education*, ECAR offers the following recommendations to optimize business process improvement efforts:

1. Designate formal resources and funding to prompt business continuity readiness activities

The study suggests that mobilizing formal resources for business continuity readiness reaps advantages. While respondents named funding as their top barrier to business continuity planning, our results suggest that it wouldn't take a huge shift in resources to make a difference in perceptions of funding adequacy. Just over one percentage point of mean central IT budget allocation for business continuity separated those who disagreed that they had necessary funds from those who agreed that they did.

2. Strive for institutional resilience.

The most advanced thinking about business continuity stresses resilience based on both redundancy and flexibility. Business continuity principles should be built into business process design from the beginning, making them an integral part of institutional practice rather than an isolated, easily sidetracked special concern. Likewise, technical business continuity solutions must rest on a firm architectural basis designed for continuity. Institutional culture should encourage individual initiative and mission dedication.

3. Deploy awareness, training, and testing as a high-impact means to strengthen readiness.

Awareness, training, and testing were the areas of greatest weakness in the business continuity readiness profiles of our respondent institutions. Taking into account fiscal and political constraint, such activities may provide the biggest bang for the buck among practical means to improve business continuity readiness.

4. Implement institutional dialogue to foster a holistic business continuity approach.

Despite the institutional nature of business continuity readiness, respondents were neutral at best regarding the involvement with business and academic units. Awareness training could provide one means to draw in campus constituencies. Another is dialogue between CIOs and CBOs, as the two groups' shared perceptions should provide excellent grounds to create an effective collaboration to support business continuity.

generally positive. They tended to rate the performance of people highest, followed by infrastructure, business continuity plans, and facilities. The relative rankings suggest that when all is said and done, institutions rely mainly on the skill and creativity of their people rather than their infrastructure and business continuity procedures.

About half of CIO survey respondents agreed or strongly agreed that their institutions were prepared to restore centrally controlled systems in the event of a disruption, and another quarter were neutral. We found statistically significant associations between higher ratings of perceived institutional ability to restore centrally controlled systems and a number of other measures, including stronger agreement that the institution had the necessary funding and staffing for IT business continuity support; more advanced IT business continuity/disaster recovery plan status and greater number of documented business continuity-related procedures; conducting busi-

ness continuity tests; and stronger agreement that central IT was involved with business and academic unit business continuity planning.

Business Officers Have More Positive Outlook

For purposes of comparison, we also surveyed business officers at NACUBO member institutions. The results from the CBO survey were uniformly (though not dramatically) more positive about institutional business continuity support than the CIO survey results. It may be that the two groups' perceptions differ less on empirical grounds and more because of their respective responsibilities and the interpretations that flow from them. The key matter for CIOs and CBOs to discuss is whether they're looking at different sets of information that need to be reconciled or are interpreting shared information in mutually appropriate ways.