Key Findings

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

Judith A. Pirani and Ronald Yanosky

One may associate business continuity (BC) planning with extraordinary events like a hurricane or an earthquake, but the reality is that challenging, disruptive events happen at higher education institutions with surprising frequency. A commonplace event like an electrical outage or an equipment failure can potentially immobilize day-to-day activities. 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 powerful financial incentives to optimize BC readiness.

BC readiness is truly an institutional activity of which IT must be an integral part. IT's role in business and academic operations has grown enormously in the past decade, and this enlarged sphere of IT dependency has created new vulnerabilities alongside new capabilities. Furthermore, distributed computing and ubiquitous networks have made the job of protecting and restoring the IT environment far more complex than it was in the days of centralized, mainframe computing. To support institutional business and academic continuity, central IT units will have to bring to bear both their traditional competencies and a new level of engagement and alignment with overall institutional goals. At the same time, IT cannot "own" BC or deliver it single-handedly.

Responding to a well-documented increase of interest in business continuity and disaster recovery issues among higher education CIOs following the calamitous hurricane season of 2005, the EDUCAUSE Center for Applied Research (ECAR) designed a study to inform administrators about how institutions approach continuity issues and to identify practices associated with good BC outcomes. As summarized below, *Shelter from the Storm: IT and Business Continuity in Higher Education* looks at many aspects of IT support for BC, including the overall institutional context, BC planning activities, the infrastructure and technologies that support BC, awareness programs and BC readiness testing, and the kinds of disruptive incidents institutions experience and how well respondents think their institutions have responded to them.

Defining Business Continuity

Traditionally, IT units have used the term *disaster recovery* (DR) to refer to their disruption planning and response activities. With a long pedigree going back to the data processing era, DR mainly focuses on achieving rapid technical recovery through data and system restoration. Our study recognizes the continuing importance of traditional DR, and, as the summary below will show, we examined many classic elements of technical recovery. 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, we see DR as part of a more inclusive paradigm: business continuity.

As we define it, business continuity refers to *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 includes additional activities. In particular, BC focuses attention on customer (student and other constituent) satisfaction; pursues a goal not just of recovery but of operational continuity during and after incidents; takes a holistic approach that includes institutional risk assessment and interdepartmental communication and alignment; and recognizes a broad range of threats beyond natural and other major disasters.

Methodology

ECAR pursued a multipart research approach to this study. We began with a literature review to identify issues and establish the research questions, consulting with a select group of CIOs and BC experts for the purpose of identifying and validating research questions.

Next we administered two online surveys, which we refer to as the CIO and CBO surveys. The first was a quantitative Web-based survey in May 2006 of IT administrators (mostly CIOs) at 340 higher education institutions among the EDUCAUSE member base. Proportionately, we had the strongest participation from doctoral institutions (28 percent of respondents). About eight in 10 respondents agreed or strongly agreed that they were personally very involved in central IT support for BC at their institutions.

To gain an alternative viewpoint on BC, we followed with a companion online survey in October 2006 of the National Association of College and University Business Officers (NACUBO) membership that covered a subset of the initial survey questions. It generated 247 responses, including 52 institutional matches with the IT administrators' survey (that is, responses to both surveys from the same institution). Respondent institutions represented the full range of Carnegie classes, though BA and AA institutions made up a relatively larger proportion than in the CIO survey. Among CBO respondents, 79 percent identified themselves as their institutions' chief business/financial officers. Eight in 10 agreed or strongly agreed that they were personally very involved with BC planning at their institutions.

Finally, we supplemented the quantitative research with postsurvey qualitative interviews with 15 executives and IT staff members involved in BC, conducted at an EDUCAUSE executive summit.

Significant Findings

The story that emerges from *Shelter from the Storm: IT and Business Continuity in Higher Education* is that IT readiness to support institutional BC is a work in progress. Our respondents clearly see BC as an important activity worth the expenditure of considerable resources. Nevertheless, IT support for BC often looks like a background process, attended to as resources and contingencies permit, rather than a focused, high-priority activity. Yet the benefits are apparent for those institutions that tackle BC readiness aggressively, for we found that institutions engaged in recommended BC best practices tend to report better outcomes.

In the following sections, we summarize and synthesize our findings. Except where otherwise specified, all findings presented here refer to the longer and more detailed CIO survey.

Institutional Context: Strong Incentives, Limited Resources

Respondents on the whole thought that awareness of the need for BC planning was high at their institutions. On our scale ranging 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. A still-stronger mean agreement (4.12) that awareness was higher than it was two years ago suggests that the dramatic hurricane seasons of 2004 and 2005 had an impact on perceived awareness.

Respondents also tended to agree that senior management placed high priority on BC planning, but when asked whether BC was one of the top three IT issues at their institutions, they averaged an unenthusiastic 2.92 response. They were downright pessimistic in assessing whether BC practices were woven into the fabric of their institutions' business operations; nearly two-thirds disagreed or strongly disagreed, and the mean response was 2.31.

While the spate of recent disasters around the globe seems to have helped drive BC planning efforts, more long-term and fundamental factors stood at the top when we asked respondents what was driving BC planning at their institutions. The two top drivers (tied for first place) were keeping current with business directions—in short, BC as business best practice—and audit requirements. Awareness of recent global disasters was the number-three driver cited. Among barriers to BC planning, the top item by far was lack of adequate funding, followed by two issues that hint at the difficulties of interdepartmental BC coordination: failure of business and academic units to define their BC needs, and the difficulty of developing campus policies and procedures.

A question we asked about reliance on IT confirmed our suspicion that, for most respondents, institutional business continuity is unthinkable without functioning IT systems. Asked their level of agreement that business units at their institution could carry out essential operations if central IT systems and services were unavailable, 68 percent of respondents disagreed or strongly disagreed.

Most respondents reported the presence of an institutional entity to handle disruptions; three-fourths reported that their institutions had emergency response teams to manage the overall response to a disruption, and almost as many reported that their central IT unit had an IT emergency response team. Aside from these response teams, we generally found institutions taking a lightweight approach to BC management. About half of CIO respondents said that their institution had designated a senior

executive who was responsible for institutional BC planning, and only 14 percent reported an institutional office for BC planning.

A critical concern of BC planning is interdepartmental communication of needs and priorities. Asked their level of agreement that central IT is actively involved in BC planning conducted by other units, respondents averaged only a neutral response (3.09 on our 5-point scale) regarding involvement with business units and a below-neutral response regarding academic units. They agreed somewhat more strongly, however, that central IT was aligned with the BC goals of such units. And they agreed more strongly that central IT is actively involved with institutional BC planners and local IT units.

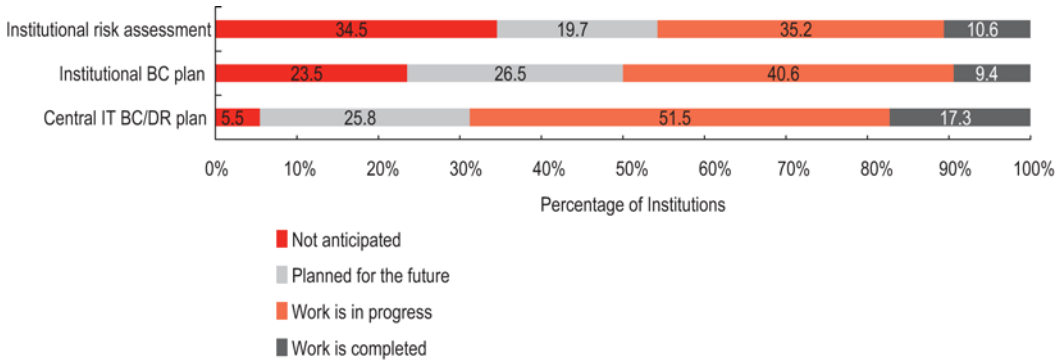
Respondents to the CIO survey were considerably more disapproving when it came to matters of resource sufficiency. Nearly seven in 10 disagreed or strongly disagreed that their institution had the necessary funding to deliver IT support for BC. Those that did agree were more likely to report completed BC plans, to conduct BC tests, to have alternate IT sites, and to give higher ratings to central IT involvement in other units' BC planning.

Planning and the Virtuous Cycle of BC Benefits

There is a widespread tendency to equate BC readiness with having some sort of formal plan. While our study confirmed that plans are indeed associated with good IT BC outcomes, our results also demonstrate the nuances that attend the apparently simple question of whether an institution "has a plan" and what that means for BC readiness. We asked about three different kinds of BC planning documents: institutional risk assessments, which identify the threats an institution faces, assess their potential impact, and prioritize the associated risks; institutional BC plans, recommended in some BC standards as an overall guiding document that departmental plans align with; and central IT BC/DR plans, which deal with IT's response to disruptions.

Those who said work was in progress made up the largest response group in each case; relatively few of our respondents told us their institutions had completed formal institutional risk assessments, institutional BC plans, or central IT BC/DR plans. As Figure 1 shows, only about one in 10 respondent institutions said they had completed one of the first two items, and about 17 percent had completed central IT BC/DR plans. While substantial numbers of respondents said they did not anticipate creating institutional risk assessments or BC plans, the overwhelming majority said they at least planned to create an IT BC/DR plan.

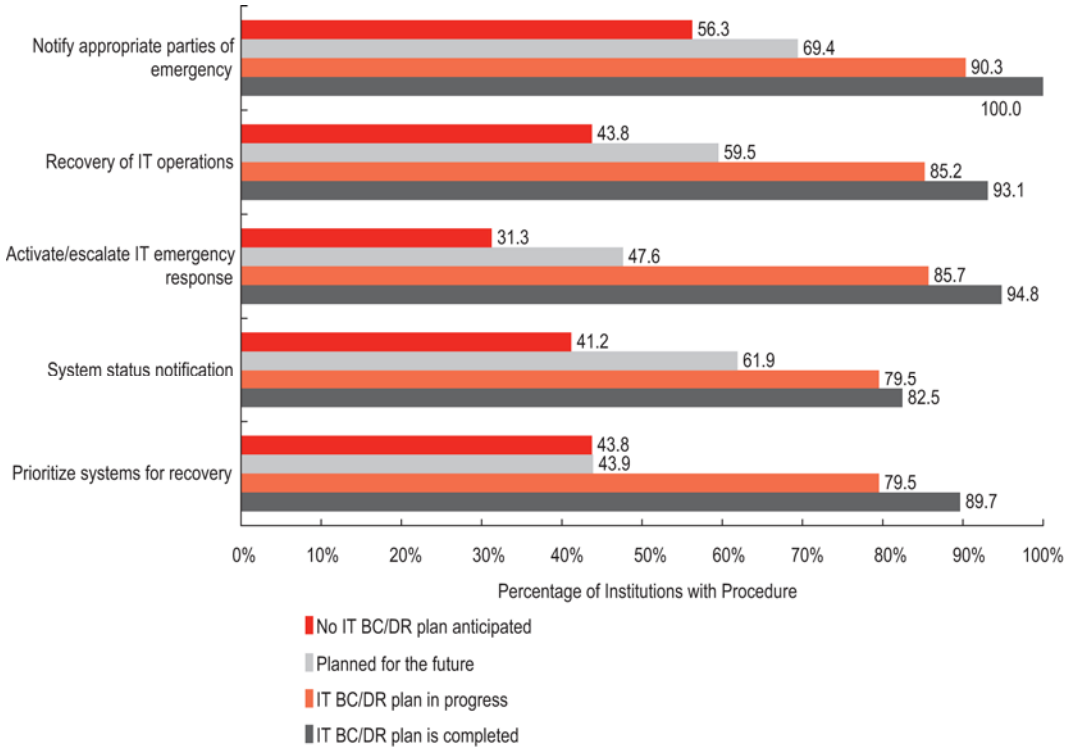
Figure 1. Status of BC-Related Planning Documents



But an incomplete plan does not necessarily imply the absence of documented BC procedures. In addition to asking about the status of institutional risk assessments and IT BC/DR plans, we asked about documented component procedures that are typically contained in them but which may also exist as stand-alone procedures. Documentation of such procedures was much more common than the risk assessment/plan completion figures imply. For example, concerning 13 different central IT procedures related to BC that we asked about, 91 percent of respondents said they had documented at least one procedure, and the median number of documented procedures was eight. Some key procedures, such as those for notifying appropriate parties of an emergency and recovering IT operations, were reported either in a plan or as a stand-alone procedure by 75 percent or more of our respondents. Thus, institutions lacking a completed plan may nonetheless have substantial documentary coverage at a procedural level.

This is not to say that bringing BC plan projects to completion has no benefits. Figure 2 shows the relationship between IT BC/DR plan status and the five most commonly documented BC-related procedures that we asked about. Those with completed IT BC/DR plans were far more likely to report having documented each procedure than those who did not anticipate creating a plan or those who only planned one for the future. In-progress institutions, however, had procedure documentation rates close to those of institutions that had completed plans.

Figure 2. Top Five Documented Central IT BC Procedures by Central IT BC/DR Plan Status



Besides the strong relationship between plan status and number of documented procedures, we also found other evidence that working on plans seems to situate respondent institutions in a virtuous cycle of benefits—though whether plans drive good actions or vice versa is harder to say. Factors

such as agreeing that BC-related procedures are kept up to date, conducting BC tests, and possessing operational alternate IT sites all tended toward better measures among those with more advanced institutional risk assessment and IT BC/DR plan status.

Backup Methods Are Diverse, but Infrastructure Redundancy Weak

We found a healthy mix of backup strategies. Although virtually all respondents reported widespread use of backup to vault-stored media, this was fortified at over half of respondent institutions by at least selective use of data mirroring and high-availability techniques.

We found a more worrisome situation when we looked at alternate IT sites that can be used when primary sites are unavailable. About three in 10 respondent institutions reported having at least one operational hot or cold site, but many of these were on or close to campus. Altogether, only about 16 percent of our total respondent base currently reports an operational hot or cold site beyond a 5-mile radius from central IT operations. A large number of in-development and planned alternate sites could reduce this exposure in the future, but for now, most institutions would have to improvise in a widespread crisis that shut down primary IT operations and the immediately surrounding locale.

The relatively low rate of alternate site coverage does not seem to be due in the great majority of cases either to choice or complacency. Most of those without alternate sites have plans to acquire them, and those that don't plan to acquire them chiefly cite lack of funding or immature BC plans as the reason.

Among assorted redundant/backup infrastructure items and services we asked about, backup power for IT sites, reported by slightly over half of respondents, was the most common. One in five or fewer said they had redundancy in place for ISPs, the institutional Web site, and e-mail, though many more in-progress and planned efforts were reported.

Awareness and Testing Need Work

BC awareness and testing were among the areas of greatest weakness in the overall BC readiness profiles of our respondent institutions. Nearly eight in 10 CIO respondents disagreed or strongly disagreed that their institutions regularly communicate BC awareness issues. Only about 35 percent of institutions reported conducting tests of IT readiness to support BC, and some of these said they carried out tests less than once per year. There was a strong relationship with IT BC/DR plan status: 74 percent of institutions with completed IT BC/DR plans said they conduct tests, far higher than among institutions reporting less advanced plan status.

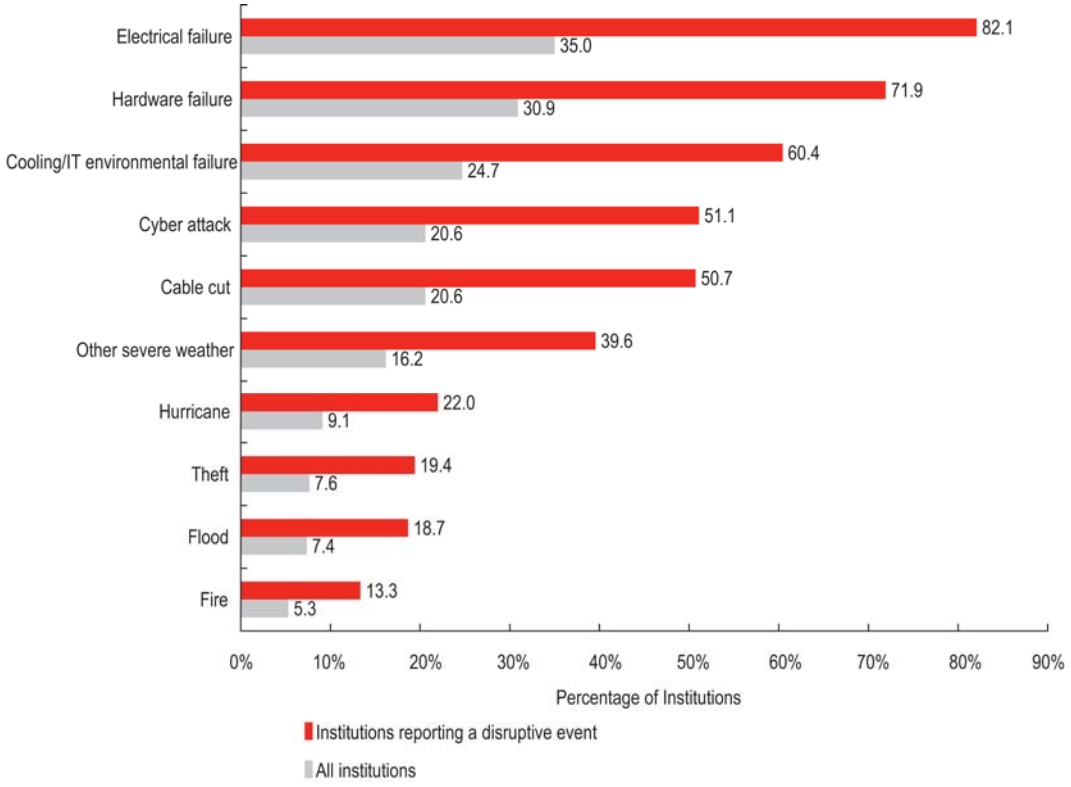
Even institutions that conduct tests often seem to have misgivings about their testing regimes. Only about one testing institution in four agreed or strongly agreed that their tests are frequent enough or challenging enough, though many others were neutral rather than disagreeing. But testing institutions are much more positive about the usefulness of tests: seven of 10 agreed or strongly agreed that they had used test results to improve BC plans and procedures.

Incident Experience and Response

Though BC planning can seem frustratingly hypothetical, many of our CIO survey respondent institutions had had occasion to discover how real institutional threats can be. About half reported that

they had experienced at least one disruption in the last five years that had triggered a central IT emergency response; most of these had experienced more than one. As Figure 3 shows, electrical and hardware failures were the most common triggering events, though weather also played a major role.

Figure 3. Top 10 Events Triggering Central IT Emergency Response in Last Five Years



Though most of the top IT emergency triggers were relatively "ordinary" events rather than the spectacular disasters that attract significant media attention, this does not mean that they always had localized effects. For the top seven IT emergency triggers shown in Figure 3, between 20 and 80 percent of events were described as having campus-wide or campus- and region-wide impact. This extent of widespread impacts strongly underscores the need for cross-unit coordination in BC planning.

Seventy percent or more of respondents experiencing disruptions reported such operationally immobilizing consequences as failed networks, unavailable business and academic applications, and nonfunctioning communications systems. Three in 10 reported losing access to primary IT facilities—a disturbing percentage given the low availability of alternate IT sites that our study found.

Despite these sometimes sobering consequences, when asked how they would assess aspects of their institution's response to the most serious disruption they had experienced in the last five years, respondents were generally quite positive. IT staff got the highest mean rating, 4.33 on a scale of 1 (poor) to 5 (excellent). Overall, respondents tended to rate the performance of people highest, followed by infrastructure, followed by BC plans and facilities. Though BC plans ranked near the

bottom of our list, respondents gave them a mean near "average" performance (3.11) rather than a poor or fair rating. The relative rankings of response performance, however, suggest that when all is said and done, institutions rely mainly on the skill and creativity of their people rather than on their infrastructure and BC procedures.

BC Outcomes and Institutional Performance

Asked to sum up their perceptions of their institutions' ability to restore systems and the alignment of IT BC support with senior management expectations, respondents were moderately positive. About half 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, producing a mean of 3.27 on our 5-point scale (1 = strongly disagree, 5 = strongly agree). They were a bit less optimistic about alignment with senior management expectations, averaging a 3.09 response.

What accounts for differences in these self-assessments of basic BC outcomes? Somewhat surprisingly, we found no significant differences in preparedness-to-restore responses on the basis of Carnegie class, institution size, public/private control, or U.S. region. But we did find 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 BC support;
- more advanced IT BC/DR plan status and greater number of documented BC-related procedures;
- conducting BC tests; and
- stronger agreement that central IT was involved with business and academic unit BC planning.

Business Officers Have More Positive Outlook

For purposes of comparison with the CIO results, we also surveyed business officers at 247 NACUBO member institutions, using a shortened version of the CIO survey. We focused much of our comparative analysis on the 52 institutions for which we had both CIO and CBO responses

For the most part, CBOs and CIOs had similar views about the factors driving BC planning. Asked to identify the top three drivers at their institutions from a list of 11 choices, the two groups gave similar answers for most items, typically within a few percentage points of one another. One major exception, however, stood out: CBOs were much less likely to choose audit requirements as a top-three driver than were CIOs. In the matched-institution groups, 31 percent of CBOs chose audit requirements as a top-three driver, making it the fifth most commonly cited item among them, while 54 percent of CIOs chose it, leaving it tied for their second most commonly cited item.

We found a pattern similar to the one regarding drivers when we asked respondents to choose the top three barriers to BC planning at their institutions. We found only one barrier item in which their differences were statistically significant: CBOs were more likely to name lack of staff expertise as a top barrier (46 percent) than were CIOs (25 percent).

Relatively few CBO respondents reported that their institutions had completed overall institutional BC plans. Reported completion rates of 10 percent among the matched-institution CBO subgroup were not dramatically different in absolute terms from the rates among CIO counterparts. CBOs did tend, however, to report more institutional BC plans in progress, and correspondingly fewer said their institutions did not anticipate creating such a plan. The fact that in-progress and planned institutional BC plans together make up two-thirds or more of both CIO and CBO responses suggests that institutions see value in such plans and want to have them.

As with the CIO results, we found a significant association among all-institution CBO respondents between having a senior executive designated for institutional BC planning and institutional BC plan status. Among CBO respondents with such an executive, 12 percent reported a completed institutional BC plan and 74 percent reported one in progress; among those lacking a designated senior executive, none had a completed institutional IT plan and 43 percent had one in progress.

To get a sense of how CBOs perceive institutional performance in real emergencies, we asked them (as we did CIOs) whether their institutions had experienced any disruptions to normal business and academic operations in the last five years that caused central IT to implement formal or ad hoc emergency response procedures. We then asked those that had been through such an experience to evaluate various aspects of the response to the most serious disruption, using a scale that ran from poor (1) to excellent (5).

CBOs were less likely than CIOs to report any such disruption: among the all-institution group, 28 percent reported a disruption triggering a central IT emergency response, versus 47 percent among CIOs. The lower response isn't too surprising, since the question was geared toward central IT emergency responses which, we speculate, would tend to be better-known to CIO respondents. The discrepancy suggests, however, that it might be wise for CIOs to ensure that CBOs have a full and accurate picture of how often the central IT unit is called upon to address disruptions.

When it came to assessing aspects of the response to the disruption, CBOs gave similar answers to CIOs; there were no statistically significant differences between the two groups. Like CIOs, CBOs tended to give the most positive ratings to people and services, more middling ratings to technology, and the lowest ratings (but still a mean 3.10 on a 5-point scale) to BC plans and procedures. In addition, CBOs gave strongly positive responses to the question of whether the central IT emergency response in question had met institutional BC objectives. In the all-institution CBO group, 75 percent said that the response had met those objectives.

Views on funding sufficiency for IT BC support presented one of the strongest disparities we found in the CBO/CIO results. Asked to rate their agreement with the statement that their institution has the necessary funding to deliver IT support for BC, CBOs and CIOs among both the all-institution groups and the matched-institution subgroups gave significantly different mean responses (see Table 1). While CIOs averaged slightly above a disagree (2) response, CBOs came close to a neutral (3) response.

Table 1. Funding Sufficiency for IT BC Support

Statement	All Institutions		Matched Institutions	
	CBO Mean* (N = 238)	CIO Mean* (N = 332)	CBO Mean* (N = 50)	CIO Mean* (N = 48)
We have the necessary funding to deliver IT support for business continuity.	2.82	2.23	2.80	2.17

**Scale: 1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree*

Percentages of agreement put these means in perspective. While 71 percent of matched-institution CIOs disagreed or strongly disagreed that they had the necessary funding for IT BC support, 44 percent of matched-institution CBOs did so, and CIOs were only half as likely to agree or strongly agree (17 percent) as were CBOs (32 percent).

CBOs were relatively optimistic about basic BC-related outcomes that we asked about, and significantly more so than CIOs (see Table 2). On the key question of whether their institutions were prepared to restore centrally controlled systems in the event of a disruption, two-thirds of matched-institution CBOs (69 percent) agreed or strongly agreed that they were, compared to about half (49 percent) of matched-institution CIOs. Though both CIOs and CBOs tended to agree that their institutions were better prepared to restore central systems than they were two years ago, CBOs were collectively more emphatic, averaging above an agree (4) response among both all-institution and matched-institution groups. And in what CIOs might see as a welcome bit of good news, CBOs also seemed inclined toward a higher opinion of IT BC support alignment with senior management expectations than CIOs did.

Table 2. Assessment of BC-Related Outcomes

Statement	All Institutions				Matched Institutions			
	CBO		CIO		CBO		CIO	
	N	Mean*	N	Mean*	N	Mean*	N	Mean*
Institution is prepared to restore centrally controlled systems in the event of a disruption.	241	3.62	333	3.27	51	3.61	51	3.08
Institution is better prepared to restore centrally controlled systems in the event of a disruption than it was two years ago.	239	4.05	330	3.73	51	4.22	50	3.60
IT capacity to support business continuity at my institution is aligned with senior management expectations.	230	3.54	318	3.09	46	3.33	49	2.84

**Scale: 1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree*

Among our CBO respondents, we found a number of the same significant associations between better BC-related outcomes and certain other variables that we found among CIOs. In particular, among all-institution CBOs, mean perceived preparedness to restore centrally controlled systems was higher among those reporting greater agreement that

- the institution has necessary funding to deliver IT support for BC;

- central IT is actively involved in business unit BC planning; and
- BC practices are woven into the institution's business operations.

In conclusion, none of the differences identified here put CIOs and CBOs in truly different universes. It may be, in fact, that the two groups' perceptions differ less on empirical grounds than because of their respective responsibilities. CIOs, hoping to maximize IT performance, may be more critical and more conscious of compromise in their BC support profiles, while CBOs, faced with a wider range of allocation decisions and BC concerns beyond IT, may feel that IT's BC activities are appropriate to a balanced assessment of institutional needs. 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.

Conclusion

Our respondents clearly see BC as an important activity worth the expenditure of considerable resources. They were at least moderately confident of their basic ability to restore systems following a disruption and believed on the whole that their institutions had performed well when confronted with real emergencies. We also found nuances that demonstrate the dangers of reducing IT BC readiness to one or two "silver bullet" measures. And we found that on the whole, institutions engaged in recommended BC best practices tend to report better outcomes.

Nevertheless, work needs to be done on BC readiness. Planned activity makes it clear that many institutions hope to make up their deficits, but because most CIO respondents (and many CBOs) disagree that they have the necessary funding to deliver IT support for BC, it will likely be a struggle for many to find the resources to realize their ambitions. To narrow the gap between BC ambitions and current capabilities, institutions will have to seek innovative ways to transform IT support for BC from an overlay to an integral part of operations. That will mean more collaboration, better leveraging of emerging virtualization and service-oriented technologies to create resilient IT environments, and a planning and budgeting approach that builds BC into every endeavor the institution undertakes.

Judith A. Pirani (jpirani@educause.edu) and Ronald Yanosky (ryanosky@educause.edu) are Fellows with the EDUCAUSE Center for Applied Research.

A copy of the full study referenced above will be available via subscription or purchase through the EDUCAUSE Center for Applied Research (www.educause.edu/ecar/).

