Draft: 2/8/2006

Collaborative Disaster Planning for AJCU Institutions

This document is intended to provide a framework for discussion of how AJCU institutions can collaborate in disaster planning. This is a work in progress, and it offers only a preliminary discussion. The AJCU campus presidents should consider the questions raised in this document and provide feedback to the Conference on Information & Technology Management (AJCU-CITM).

Executive Summary

While there are some opportunities for collaboration in such areas as best practices, emergency web deployment, making computer room space available, and consortium purchasing of disaster services, each campus will be largely responsible for its own disaster plan. Each institution must find its own comfort level with the safety net that it is willing to purchase. Purchasing disaster services is like purchasing insurance. Nobody can point to a tangible benefit because they have an adequate insurance policy. The payoff comes in the unlikely occurrence of the event for which you purchased the insurance.

Background

There are a number of reasons why institutional business continuity and Information Technology (IT) disaster planning have taken on new importance:

- Hurricane Katrina and 9/11 impacted institutions of higher education very directly. Catastrophic events, though unlikely, do happen.
- As time passes, more and more business and instructional processes are dependent on computer and information technology. Arguably, instruction is just as dependent on email, web access, and course management, as the business office is on payroll and the registrar on the student registration system.
- Federal privacy regulation requires that protected data (e.g. bank account numbers and social security numbers) remain protected during a disaster and that institutions have plans in place to protect the information.

What are AJCU institutions doing now for IT disaster planning?

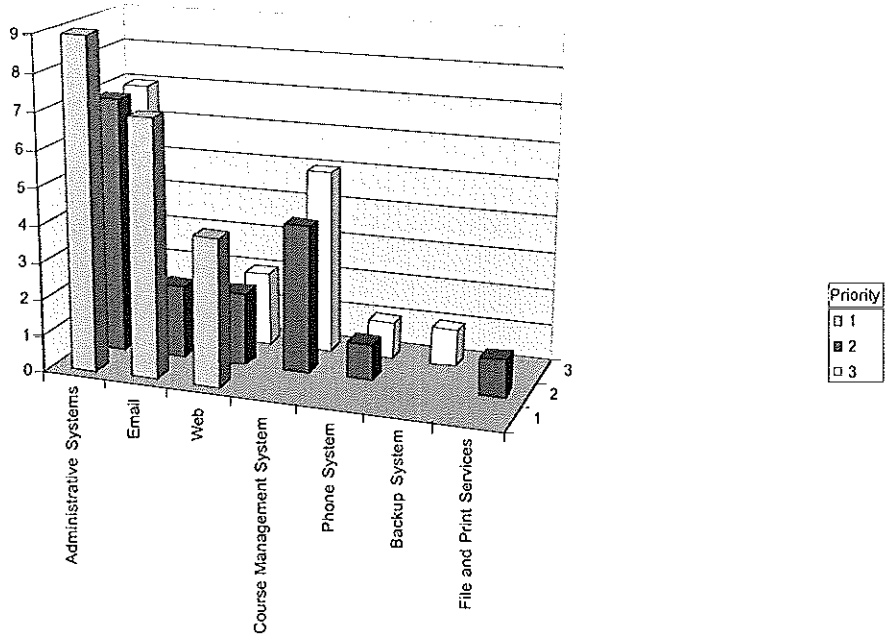
In recognition of the potential for collaborative IT disaster planning, in September 2005 Richard Valente of John Carroll University solicited interested Chief Information Officers (CIO's) of CITM to collect information about disaster planning on AJCU campuses and to make recommendations for improvement. Brian Young of Creighton University agreed to chair a working group.

Brian and the working group released a survey for CITM membership in January 2006. The survey queries the current status of campus business continuity and disaster planning, including i) whether the campus has a tested IT disaster plan; ii) what the

perceived level of support was for an IT disaster plan; iii) what sorts of disasters were perceived to be most likely; iv) and a list of prioritized computer applications that were most critical.

Ten institutions responded. As might be expected, perceived threats are linked to geography. Nobody in Buffalo is too worried about a hurricane. The responses on identifying the most critical systems to recover are shown in Figure 1, Administrative systems (e.g. student information system, payroll, etc), the campus web site, electronic mail, and the campus course management system (e.g. Blackboard or WebCT) are perceived as the most critical systems.

Figure 1: Which Systems are Most Critical for Recovery?



Will a collaborative approach substitute for individual campus planning?

The most likely failures are not catastrophic, and recovery strategies will most often be local to a particular campus. This means that plans for restoring IT services after a limited local disaster (fire, flood) are at least as important as preparing for a Katrina style, widespread disaster. Each campus must determine relative importance of restoring each of the many computer-based services (web services, administrative functions, email, course management and library systems, etc.) Each campus must exercise and test good backup and recovery procedures. For such local failures, relying on facilities or services beyond what is in direct campus control is likely to cause extra delay and expense even with tested procedures for doing so.

What are the constraints on IT Disaster and Recovery?

Though several AJCU institutions use the same components of their information processing systems, no institution is configured to absorb the work of another institution. For example, the majority of AJCU institutions run Banner, but each Banner institution has developed its system for a single campus, namely its own, and that another campus runs Banner has little direct impact on disaster planning.

As computers have become smaller, more powerful, and more specialized, the numbers of computers that must be considered in planning for disaster recovery has mushroomed. In the "old days," a large central computer processed the campus workload, and restoring services meant loading backup tapes of software and data on a single similar system. Today, there are many specialized systems with a variety of hardware and software configurations that vary significantly from one campus to another, even among those that use the same major software components. For example, one type of specialized computer is the computer that performs backup of the other computers' information. Billions of characters of information must be transmitted over a high speed network for the backup to be completed. Another type of specialized computer is used to route electronic mail to the proper person. There are numerous examples of inter-computer communication that require high speed and high capacity networking. This type of network is ordinarily available and affordable only on computers that are directly connected by fiber optic cable. This is typically limited to a campus.

Another characteristic of modern computer systems is that access to them by computer users is online. For example, a student registration system is of little use without the ability of students to connect to it through their personal computers. Such communication may be from the on-campus network, but access through the slower speed Internet is satisfactory for human to computer interaction. Online availability is usually 24 hours a day, seven days a week. Again, this complicates any planned sharing of similar equipment and systems.

What all this means is that for a university to recover normal computer operations, it needs a computer environment in which computers can talk to each other at extremely high speeds and that the entire environment is available online to its users though the Internet.

There are separable parts of the system that could operate more independently, for example, a backup web site. But for most campus computer processing, a backup computer site is required into which the most critical computer systems can be installed, connected to one another with fiber optic cable, and connected to the Internet. The backup site needs to have space, power, and environmental control. There must be a way to transport backup to the site, even during a crisis, or alternatively, the backup site's data must be kept synchronized with the primary site.

Joel Cohen 2/8/06 11:19 AM
Deleted:

So one conceivable way for institutions to help each other is to provide such an environment into which an affected campus can place equipment, either pre-positioning

the equipment (a "hot site") or ready to accept equipment that is acquired on an emergency basis after the disaster strikes (a "cold site"). Such an approach begs the question, can a commercial service in which the risk is spread to more institutions accomplish this more cost effectively?

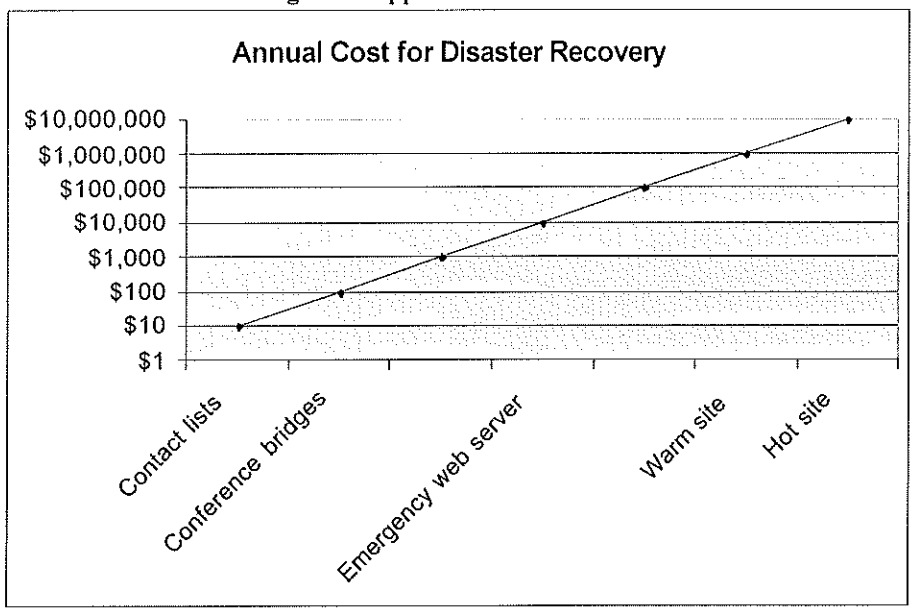
What sorts of commercial disaster recovery services are there?

Commercial services can provide a hot site. They can also provide a "warm site," that is, deliver a trailer with equipment that can run the prioritized computer systems. The equipment is not necessarily identical to that owned by the campus, but one of the strong points of commercial based systems is that the recovery procedures are thoroughly tested. Indeed one of the strongest arguments for a commercial service is that the recovery procedure is so detailed that even in the case that university personnel are not available for recovery, commercial service personnel will effect the recovery. Commercial services are subscription based; though the vendor has to purchase a certain amount of equipment, the university can make a multi-year commitment at a fixed cost. If a disaster is "declared," there are typically activation costs. Training and testing of disaster recovery plans are crucial, on at least an annual basis; some of the testing would take place at a vendor site.

What do disaster recovery services cost?

There are a number of options for disaster recovery plans. As might be expected, the more complete the plan the higher the costs. Figure 2 models costs versus capability and shows approximate costs in orders of magnitude. Some action items are rather inexpensive. For example, it costs little to distribute emergency contact information of key personnel to other key personnel. Such information should include alternative telephone numbers and email addresses. Similarly, conference bridges could be set up in advance so that decision makers could have audio conferences without relying on the campus communication system. For a reasonable amount of money, an alternate web site at an off-campus location can be established. This could have information that describes the campus event and perhaps has a registry where members of the community can "check in." From there it gets progressively more expensive as more servers are included and the state of readiness increases. A key question that each campus must answer for itself is, "what level of readiness does my campus require, and what are we willing to pay for it?"

Figure 2: Approximate Annual Cost



What is the AJCU CITM working group doing now?

As noted above, the group has compiled preliminary information about disaster planning status for the various AJCU campuses. We have begun to investigate what other, non-AJCU campuses are doing in this regard, particularly related to inter-institutional cooperation for disaster planning. Of course, we will share information on emergency planning with a goal of establishing a plan template. We will also make inquiries from major vendors about whether consortial pricing would significantly reduce the cost of providing emergency service sites (hot, warm or cold) for AJCU institutions.

What does the working group need from the Presidents?

It would be extremely helpful to get a sense of how many institutions would be interested in being part of a consortium, and the rough level of annual expenditures the Presidents would consider reasonable for providing some of these services. This is essentially an "insurance" question, and some consultation with each institution's risk management office may be appropriate.