**EDUCAUSE 2011 ANNUAL CONFERENCE**

***Business Continuity Management Discussion***

**Questions:**

* **How can I sell BC/DR to my institution?**
* **What are the challenges of BC and DR in a large institution?**
* **My institution does not have a business continuity plan. I’m looking for some insights and ingredients to start one.**
* **My institution has a disaster recovery plan; we need a business continuity plan.**
* **I’m interested in best practices with business continuity and disaster recovery planning.**
* **I’m building a stealth BC/DR plan at my institution. What are the essential elements of both?**
* **I see the path to creating business continuity and disaster recovery plans. How do I keep them fresh, alive, and tested once I have them?**
* **I’m interested in opinions on the value of business impact analysis and insights on how to accomplish it.**

**EDUCAUSE 2011 ANNUAL CONFERENCE**

***Business Continuity Management Discussion***

**Group 1 – The Cloud is Changing the Rules of the Game**

* What challenges will there be to accomplishing disaster recovery if, as predicted, cloud services become more interrelated and dependent on each other in the future?
* Do you feel that moving services to the cloud will simplify or strengthen business continuity/disaster recovery planning?
* What do you see as the chief risks of moving to the cloud relative to business continuity?

**Notes:**

* The Cloud presents a different kind of risk. It could promise better services, but how do we verify the capabilities of, and ability of providers to deliver?
* The perception is that risk in the Cloud is less environmental (susceptible to hazardous events) and more process and security focused (ability to deliver, ability to keep secure).
* The Cloud presents heightened risk stemming from contractual aspects. Not just what can or can’t be negotiated, but unforeseeable consequences as well.
* Disaster recovery of high performance computing. How do you recreate that?
* From a disaster recovery perspective, where will new infrastructure come from? Vendors are eager to help in a hazardous event. There may be difficulties in a large scale event though as the means of transport are typically under tight control of the government or military.
* Moving email to the Cloud is an option many institutions are availing themselves of. The perception is that disaster recovery is not considered to be a significant factor in the decision.
* Institutions may lose control over the service levels when they are moved to the cloud.
* Institutions may lose the ability to improvise solutions in the case of an event involving a service that has been moved to the Cloud.
* When you move services into the cloud you likely will have little influence over change management. Requiring certified audit instruments such as SSAE 16/SAS 70 can provide some confidence in the Cloud provider depending on what areas the audit covered.
* The personal computer era created new challenges for business continuity and disaster recovery; the Cloud era will increase the problem exponentially.
* With in-house solutions we have close oversight of all aspects of a solution. In order to gain that same level of trust, institutions will have to develop the same close oversight relationship with cloud providers to overcome the loss of control.
* Fractured networks and the lack of a consistent set of protections may present a unique form of risk.
* Institutions should negotiate contacts carefully and build safety nets for institutional data.
* The business failure of a Cloud provider poses as significant a risk as an environmental disaster.
* Even large firms may not always deliver on their promises in the Cloud.
* Institutions must identify exit strategies for any Cloud solution they engage. Google does not provide an easy way to pull your data out if you decide to switch.
* The risks of the Cloud can be mitigated to some extent by utilizing a hybrid private/public cloud.
* An institution’s business continuity planning should consider and address the loss of personnel following a hazardous event.
* Pandemic planning raised the issue that you cannot plan for and address the loss of personnel in every eventuality. At some level of staff loss the institution will be forced to cease operations. Katrina cited as an example of the scattering of personnel.

**Group 2: Accomplishing Meaningful BC/DR Planning and Testing**

* How successful has your institution been with business continuity/disaster recovery planning?
* What can be done to achieve more buy-in from campus units?
* Do tools (e.g., Kuali Ready) help business continuity/disaster recovery planning efforts? Is your institution using a tool effectively today?

**Notes:**

* The testing of business continuity and disaster recovery plans plays a major part in the process of improving them as each test brings out new issues that need to be addressed.
* Unfortunately, in most cases significant real events are required to raise the BC/DR issue to the surface.
* At what level do other institutions develop their plans? Plans for each application; each business unit; or a single institutional plan? Consensus appears to be that it is normally at the business process level.
* What is the definition of business continuity? Are there two separate aspects to business continuity; business process and IT aspects?
* How do you draw the attention of campus units to business continuity? Still a problem. IT still tends to drive it, but where is the business participation?
* How do you get the buy-in? Unfortunately from a significant emotional event.
* LSU developed an emergency operations center (EOC) after Katrina. How about other institutions? Several formed them as well in the wake of 9/11.
* Getting attention for business continuity planning: use scenarios to raise awareness. Desktop exercises are moderately effective.
* Business units are gun shy of business continuity planning. Try to build this planning into business planning mechanisms for new processes and services.
* IT doesn’t own business continuity, but it keeps falling to IT since technology is present in most business processes.

**Group 3: BC/DR When Budgets are Tight**

* Are there ways to make up the shortfall in disaster recovery planning and measures through institutional collaboration?
* Do you have business continuity/disaster recovery planning agreements in place with local government, public safety officials, or other universities?
* What strategies has your institution used to enhance or maintain the status quo with business continuity/disaster recovery planning during the budget downturns?

**Notes:**

* Virtualization provides choices in moving infrastructure prior to warned events and for recovery following an unforeseen event. Cost savings from virtualization can be leveraged for improving an institution’s disaster recovery stance.
* Disaster avoidance and risk analysis can reduce costs by reducing the incidence of hazardous events.
* Do any institutions have reciprocity agreements in place? Some agreements are in place with no issues, but no one reported a case where a reciprocity agreement was activated.
* There is too much political “crap” to get effective reciprocity agreements in place.
* Anyone using Kuali Ready? No. Penn is using Shadow Planner.
* Software tools are not solutions to business continuity in and of themselves. They do allow institution’s to prompt process owners to update plans.