



UCLA Disaster Recovery Planning Case Study

Don Worth, Director Admin. Info. Sys.
Sue Abeles, Asst. VC CFS, Controller
Jack Ewart, Data Center Director
Karen Melick, Systems/Network Director

Corporate Financial Services

Business Continuity Planning-A “Real Life” Example

- Came to appreciate need for Business Continuity Planning through real life experience
- Experienced first in a series of power outages in our off-campus location in 1998
- Power provided by City of LA Dept of Water and Power; no local control
- One outage lasted several days
- No emergency plans in place; no backup electricity in building beyond emergency lighting; work still needed to get done
- Corporate Financial Services is responsible for core business services at UCLA

Corporate Financial Services

Business Continuity Planning Response Issues

- Were allowed only limited access to building/offices for safety reasons
- Had to assess work priorities for duration of outage
- Had to identify necessary files, other materials, etc. for relocation that we needed access to
- Required us to quickly relocate essential employees to other parts of the campus to access mainframe systems
- Had to make decisions about essential personnel and who to send home
- Work from home only an option for limited staff with direct access to mainframe as network was also down
- Had no immediate way to let customers know why we were not responding to phones and email or where we were relocating

Corporate Financial Services

Business Continuity Planning Response

- Conducted a “post mortem” of our response
- Identified need for more formal plans
- Convened a work group within CFS to prepare for next emergency
- Work Group made recommendations including need to:
 - Negotiate “agreements” with other departments to use their computer labs for access in case of emergency
 - Develop CFS telephone tree to ensure everyone gets communication and instructions; update and test tree periodically
 - Develop response matrix based on duration and scope of emergency
 - Identify “Required Function” and “Service/Access Required” for each CFS department
 - Identify critical time periods
 - Share response matrix at departmental staff meetings
 - Periodically update response matrix to address contemporary needs

Corporate Financial Services

Business Continuity Planning Response Matrix

- Functional Requirements by Department
 - In the Event of a Building Emergency Shut-down
 - In the Event of a Campus Emergency Shut-down
- Identified Required Functions and Critical Timeframes (i.e., payroll deadlines, etc.)
- Identified Resources Needed to Perform Function (i.e., access to systems, files, check stock, personnel, other assets)
- Considered Needs in Context of Length of Shut-down (1-2 days versus more than 2 days)

CFS and AIS: Formalizing Disaster Recovery and Business Continuity Plans

- Local “emergencies” provided impetus to initiate conversations in the business units
- AIS had been trying to get funding for disaster recovery without success
- 9-11 reinforced the need for a plan and funding
- Began to develop a more formalized and coordinated approach to planning

UCLA Disaster Recovery Planning History

- 05/2001: Developed Initial Disaster Recovery Plan
 - Used UCSD Business Continuity Document as pattern
 - Used existing AIS staff and Infrastructure funds (minimal)
- 07/2001: Performed limited test of Payroll at UCOP
- 09/2002: Essential application functions identified by UC Controllers:
Disbursements (Payroll, Financial Aid, AP, Sponsored Projects A/R)
- 2003: Business Continuity Plans developed by functional owners using systemwide template
- 04/2003: Established D/R contract with IBM (campus funding provided)
- 11/2004: First test at IBM, Boulder, CO:
Operating System and Network connectivity
- 04/2005: Second test in Boulder:
Successfully tested all “essential” mainframe application functions

Disaster Recovery Site Contract

- IBM contract primarily for mainframe recovery
 - \$75,000 per year
 - One 48 hour test per year
 - Local facility with 24 workstations
 - Access to their site in Colorado after a disaster (maximum 6 weeks)
 - Daily charge in an actual emergency is \$4000/day
- No arrangements yet for non-mainframe servers (not required for initial scope)

Backup Strategy

- Daily:
 - Full volume backups of mainframe environment sent to local Iron Mountain facility
 - Incremental backups of server environment sent to local Iron Mountain facility
- Weekly:
 - Full backups of server environment sent to local Iron Mountain facility
- Monthly:
 - Full volume backups sent to Iron Mountain facility in Arizona
- Storage costs approx. \$25,000 per year

Business Continuity Data Center Investments

Completed:

- Physical Security (Thumbprint, Windows, Fire doors)
- Fire Suppression System

In Progress:

- Fully redundant (and higher capacity) A/C
- Motor Generator and additional UPS

Total Cost = \$2.3M over 4 years

Work in Progress

- Emergency Email System (in production)
- Emergency Web Site (replaces www.ucla.edu)
- Next test at IBM with IBM doing the installation
- Adding additional applications to the plan (financial/FAM systems)
- Leverage UCOP risk assessment
- Business Impact Analysis for campus wide applications
- Redundant sites for ultra-critical systems (emergency web site, emergency email, authentication)
- D/R discussions at JDCMG meetings

Lessons Learned

- Need full commitment of Business Partners and Management
- Disaster recovery and business continuity take significant resources, both people and money
- Non-mainframe servers are difficult and expensive to recover
- Don't try to do too much in your first test
- Invest in technology to help recovery effort (hardware/software)
- Make D/R part of daily business
- Development of comprehensive plans requires several iterations; need to challenge assumptions
- Don't underestimate the need for communication and the confusion that will ensue in a real emergency
- Need to continually update and test plans given changing environment



Questions?