

Assessing Risks of Information Technology – *Disaster Recovery in a University Environment*

Katina Blue

Director

NC State University
Business Continuity & Disaster Recovery



History



- 1987: Data Center Improvements
 - Upgraded Fire Suppression System
 - Modifications to minimize water damage
- 1993: Recovery of Mainframe Environment and Applications
 - All applications were on the Mainframe
 - Project completed in 1996 due to limited to limited staff
 - Mobile Recovery Unit Contract and Equipment Quick Ship

New Business Driver



- Single Point of Failure
 - Data Center and Main Distribution Feeds (MDF)
- Accounts Payable Audit Finding (1st time)
 - Inability to recover HR & Financial Systems
 - Required to identify and implement a disaster recovery strategy for campus wide Disaster Recovery and Business Continuity
- Due Diligence

Business Case



- How NC State University arrived at their plan
 - Hired a Business Continuity Consultant
 - Laid out a project plan
 - Identified RTO/RPO and risks via a BIQ
 - Benchmarked with other Universities
 - Brought in vendors to assess alternatives
 - Researched best practices
 - Developed alternatives with associated costs and presented to management
 - Interim solution and long term strategy a compromise between desired state and available funding
 - Hired a Full-time Disaster Recovery Coordinator

Risk Assessment



- Identify Threats and Vulnerabilities
- Compare probability of occurrence to impact
- Performed at least bi-annually

NC STATE THREATS



- Hurricanes (*Fran, Floyd, Isabelle*)
- Flooding (*natural and human threats*)
- Embezzlement
- Power Outages
- Thefts
- Loss of Critical Staff
- Data Center (Old Insurance Bldg) that Often Floods
 - Risk Controls:
 - 3 major Data Center upgrades
 - fixed the draining in the computer rooms
 - Installed new windows and Emergency Generator

Threats Realized at NC State



January 2003 Ice Storm



August 2003 Flooding

The Data Center!

Defining Strategies



- Develop mitigation strategies based on Risk Assessment and Business Impact Analysis results using:
 - Vendor Resources
 - Reciprocal agreements between campus'
 - University Benchmark data

Researching Vendors



- Identify Vendors of DR/BC services
- Utilize
 - The Internet
 - Disaster Recovery Magazines
 - *Disaster Resource Guide*
 - *Disaster Recovery Journal*
 - *Contingency Planning & Management*
 - Other Universities and Agencies

Gather Vendor Data



- Distribute a Request for Information (RFI)
- Analyze/Rank Vendor Competencies
 - Schedule vendor presentations
 - Conduct telephone interviews
 - Review white papers and product literature
 - On-site tours
 - Attend free technical workshops

IT Strategies: *Mobile Recovery*



IT Strategies: *Cold Site*



- A backup site that contains physical space but none of the infrastructure needed to resume operations quickly.

IT Strategies: *Warm Site*



- A backup site that is prepared for systems restoration that does not contain all of the components necessary to do an immediate restore of all business functions.
- In the event of an emergency, the hardware and software additions needed to get the system operational may cause a delay.

IT Strategies: *Hot Site*



- A backup site that is fully prepared to resume business operations immediately in the event of a disaster, including all the needed infrastructure, space and equipment.

Hot-Site



IT Strategies: *Equipment Rental*



NC State IT Strategies



- Failover power grid
- UPS
- Generators
- Secondary Data Center (hot site)
- Interim Recovery Location (warm site)
- Mobile Recovery Units
- Computer Equipment Rental
- IT Incident Reporting Database

NC State Business Strategies

- Generators for critical facilities
- Reciprocal Agreements
- Heightened security measures
 - Card Access
 - Closing of Public Entrances
 - Requirement of ID Badges
 - Security Guards



Identify Recovery Teams



- Technical Recovery Teams
 - Mainframe Team
 - Distributed /Web Team
 - Communications Team (Data/Voice)
 - Emergency Response Teams

Testing/Exercising the Plan

- Technical Walkthroughs
 - Include recovery team members
- Management Operations Center Exercises
- MOCK Exercises
- Tabletop Exercises
- Recovery Strategy
- Communications System



NC State Tests and Exercises



- Annual Mainframe Recovery Test
- Annual Distributed Environment Test
- Disaster Recovery Activation Drill
- Automated Dial Out System Test

Test Use Case



- Financial Aid Server Failure
 - Multiple drive failure prior to nightly backup
 - Lost a day's work
 - 95% was restored
 - Customer commentary/notes lost
 - Value of BCP recognized
 - Improved processes implemented
 - Model for other business units

Documenting Tests



- Expectations
 - Detailed list of expected results
- Results
 - Actual vs. Expected
- Lessons Learned
 - What will make future tests more successful
- Comments/Suggestions
 - Improvements to the process



- In 2002, NC State expanded Disaster Recovery for Information Technology to include Enterprise Business Continuity/Disaster Recovery Planning

NC State IT Disaster Recovery

Disaster Recovery of **C**entral Computing & Communication at NC State University

The University's obligation to its major stakeholders requires that we develop and implement a combined academic and administrative Disaster Recovery Plan (DRP) to ensure that the risk of major disruptions to critical University processes have been mitigated. The DRP will endeavor to support all mission critical business processes that may be impacted by the loss of central computing and communications. A critical component of the DRP will be the development of a viable Business Continuity Plan (BCP) for critical University offices and services which will help ensure that the gap between the loss of IT services and recovery of normal business operations is adequately addressed for all University organizations.

To oversee this effort, a [Disaster Recovery Oversight Committee](#) has been established. Steve Keto, Associate Vice Chancellor of Resource Management and Information Systems, and Sam Averitt, Vice Provost for Information Technology, will serve as co-chairpersons. The Committee will oversee and effectively coordinate the implementation of the recovery efforts.

Contact Information

- [Project Information](#) Disaster Recovery Coordinator (919) 513-2033 or (919) 389-2882
[Monica Mauk](#)

<http://www7.acs.ncsu.edu/drproject/>

Manager, CSU 117032
[Joe Cosgriff](#), Assistant Director of Information Security

NC State BC/DR Department

NC STATE UNIVERSITY

Environmental
Health & Public Safety
Center

[Index](#)

[MSDS](#)

[Training](#)

[Emergency Info.](#)

NC State University
Business Continuity & Disaster Recovery



Our Mission is to provide leadership in coordinating, assessing, developing and communicating business continuity planning principles to campus departments and colleges (including education on developing Business Continuity Plans) to ensure the continued operation of critical processes, resource and asset protection, and loss mitigation in the event of a disruption.

The Director's Corner

[History](#)

[Chancellors' Mandate](#)

[What is "MISSION CRITICAL"](#)

[UNC Office of the President Requirement](#)

[Join the BCP listserv](#)

[BCP Regulation](#)

[BC/DR Planning Committee](#)

[Department Objectives](#)

[Cohorts and Coordinators](#)

[BCP Phases](#)

[Planning Templates](#)

[IT Disaster Recovery](#)

[Campus Presentations](#)

[Helpful Links & FAQ](#)

<http://www.ncsu.edu/ehs/bcp>

Successful Program



- Risks are identified and assessment findings are agreed upon
- Business Continuity Plans are written, maintained, and tested
- Staff is trained and educated on an ongoing basis

Contact Information

Katina Blue

Director of Business Continuity

919-515-5201

katina_blue@ncsu.edu

NC State University
Business Continuity & Disaster Recovery



Helpful Links

<http://www.ncsu.edu/ehs/BCP/bcp.htm>

- *NC State Business Continuity/Disaster Recovery*

<http://www7.acs.ncsu.edu/drproject>

- *NC State Disaster Recovery of Centralized Computing and Communications*

<http://www.drj.com>

- *Disaster Recovery Journal*

<http://www.contingencyplanning.com>

- *Contingency Planning & Management*

<http://dri.org>

- *Disaster Recovery Institute*