IT DR Within the Framework of Business Continuity Planning

October 31, 2008

In the beginning ...
"Need a DR Plan."

Auditors
Strategic Planning
Tactical Planning
Board Inquiry
Best Practice

Disaster Preparedness

BEFORE

• DR plan was IT myopic
• Planning was limited in scope
• Planning was developed in silo’s
• Planning driven by opinion, perception, and budget constraints

In the almost beginning ...
A voice says,

“So, it will take “X” long to recover our primary administrative system.
Can the University deal with such an interruption?”

BCP is Multidimensional

Holistic Approach to Crisis Management
• Threat, Risk and Vulnerability Assessment
• Emergency/Rapid Response
• Business Continuance and Resiliency
• Business Recovery

Would the DR plan meet business needs?
What plans must IT have?
What plans does FDU need?

HOLD EVERYTHING
In the beginning ... "Write it up."

**Disaster Preparedness AFTER**
- Learned the distinction between Disaster Recovery and Business Continuity
- Recognition that IT DR must be driven by real business requirements and not by perception
- Recognition that an IT DR plan is one component of a larger business resiliency program
- Planning to sustain business operations extends into the far reaches of the business, not just out to the data center

**Causes of Unplanned Downtime**

<table>
<thead>
<tr>
<th>Cause</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disasters</td>
<td>42%</td>
</tr>
<tr>
<td>Utility Failures</td>
<td>23%</td>
</tr>
<tr>
<td>Other</td>
<td>21%</td>
</tr>
<tr>
<td>Hardware Failures</td>
<td>7%</td>
</tr>
<tr>
<td>System Errors</td>
<td>4%</td>
</tr>
<tr>
<td>Operations Overrun</td>
<td>3%</td>
</tr>
<tr>
<td>Application Errors</td>
<td>2%</td>
</tr>
<tr>
<td>User Errors</td>
<td>1%</td>
</tr>
</tbody>
</table>

**Historical Facts**
- 40% of small businesses will go out of business if they cannot get to their data in the first 24 hours after a crisis. – Gartner
- 43% of companies never resume business following a major fire. Another 35% are out of business within 3 years. – U.S. National Fire Protection Agency

**Lessons Learned**
- Plan a backup site in advance
- Gotchas in the details…and chargers.
- Choose a low threat data center location.
- Layer on communications methods
- Create a mirrored infrastructure.
- Even the best laid plans …
Tulane University’s IT team was able to recover its backup tapes, but the New Orleans data center was without power, and no backup site had been prearranged.

NOW: Signed on as a SunGard customer, the university is entitled to a mobile data center that could be used for local processing. And backup tapes are now sent to Baton Rouge three times a week.

When Hurricane Katrina devastated the Louisiana coast, a lack of batteries and power had Hard Rock Hotel & Casino employees relying solely on text messaging to communicate.

NOW: As part of its revamped disaster recovery plan, IT employees carry car chargers for their cell phones. There’s a new personnel plan for disasters, too.

During Hurricane Katrina, Hancock Bank’s Gulfport, Miss., data center, just one half mile from the Gulf of Mexico, was devastated.

NOW: The bank’s new $16 million data center is still in Gulfport, but the hardened, lights-out facility is located farther inland on the highest point in the area. It can withstand 200 mph winds.

An telecommunications company began to fail as the hurricane approached. Microsoft found that different telecommunications companies were failing in an order.

NOW: Microsoft disaster recovery teams learned that the best way to keep communication channels open among employees was to use a mix of cell phones and Blackberry devices with different carriers.

During Hurricane Gaston stalled over Richmond, Va., for hours, Estes Express Lines’ first-floor data center was awash in four feet of water. Company executives watched helplessly as 185 terminals used to direct the operations of more than 20,000 tractor trailers just died.

NOW: Estes pieced together a new infrastructure, complete with software that allows data to be whisked off-site immediately. That new architecture is mirrored in a hurricane proof backup site in sunny - and dry - Mesa, Ariz.

Houston-based OYO Geospace suspended all operations at its Houston facility late Thursday evening, September 11, 2008, when ordered to evacuate. High winds from Hurricane Ike caused significant damage to the greater Houston area power grid and the company’s Houston manufacturing facility lost electrical power early Saturday morning.

NOW: Power was restored Monday, September 22, 2008.

Could your organization survive a pandemic?

The World Health Organization says it is not a matter of ‘if’ but a matter of ‘when.’

Could happen within the next 200 years … or within the next 200 hours.

Are You Prepared?

Could you operate during a pandemic?

3,000 financial services organizations had a Pandemic drill during September of last year and found they could operate … but

1. The drill revealed significant stress points throughout the entire industry.
2. Recovery plans laid the groundwork for employees to telecommute but the existing infrastructure couldn’t handle the increased traffic.
3. The Internet is going to slow to a crawl … then it will go down.

Are You Prepared for Econtamination?

The points are ....

1. Stuff has hit the fan before and stuff will hit the fan again.
2. Disasters come in a variety of flavors.
3. Business Continuity (BC) is more than IT DR and Crisis/Response Management.
4. Business Continuity and Resiliency is about resuming and maintaining business operations in the face of adversity and/or while other areas of the business are being recovered.

Poll: Raise your hand if ...

- your organization has an Emergency or Crisis Management Team and/or has rapid response/notification technologies deployed
- your organization also has current, documented, and tested IT DR Plans
- your organization has formalized business continuity capability over and above the first two
Typical Preparedness Focus

- Emergency Response
  - Response Teams
  - Response Plans
  - Mass Notification Systems
  - Training, tabletops, drills

What is the business expected to do ‘during’ an extended crisis and how?

Disaster Recovery Plans
- IT Systems
- Communications
- Network

I suspect ...
- Safeguard people, property, and brand
- Deliver the appropriate internal and external messaging during the event
- Continue to conduct the mission of the enterprise with a minimal disruption to the delivery of products and services
- Maintain the flow of revenue
- Work towards the resumption of normal operations

How are you going to do this?
- Wait for the event to occur and then begin the development and implementation of methods and procedures to continue operations?
- Plan for a business interruption and have proven, documented, and tested methods and procedures in place to continue business operations.

Brain Fodder ...
- What if an incident prevented access to key locations around your campus?
  - No access to systems
  - No access to records
  - No access to files
- Suppose a serious fire destroyed your data center?
- Suppose other campus infrastructure was seriously damaged?
- What if key staff suddenly became unavailable?

Brain Fodder ...
- What if this situation was going to continue for 30 days?!
  - How might such a series of events impact your institution’s ability to carry on its academic and administrative missions?
  - At what point in time does the business of running the institution become jeopardized?
  - How would you prioritize systems restoration?
  - How would you prioritize functional restoration?

Would an extended disruption
- affect your institution’s ability to continue business operations?
- affect your institution’s ability to meet the academic needs of your students?
- affect your institutions ability to meet the needs of staff and faculty and stakeholders?
- have detrimental financial and/or enrollment impacts?
- affect your institutional reputation?
- negatively affect your career?
How is it you know this?

- Someone told you?
- You told someone?
- Experience?
- Hearsay?
- Anecdotal Evidence?
- Personal Biases?
- Gut Feeling?
- Facts based upon detailed business needs analysis?

And if you don’t know, how can you …

- be sure that any preparedness plan will meet business recovery requirements?
- develop contingency plans that actually meet the real, not perceived, need?
- spend scarce DR dollars judiciously?
- have confidence that plans will truly minimize the chaos surrounding an unfortunate event?

Answers come from Business Contingency Planning

A coordinated strategy involving plans, procedures, and other measures that enables business continuity and the recovery of processes, systems, and business operations after a disruption.

- Performing some or all affected business processes using alternate means
- Restoring operations using alternate sites, equipment, or procedures

Contingency Planning Requires

- an understanding of true business tolerances against business interruptions
- the identification of risks and plans to reduce and mitigate those risks
- balanced strategies to meet the institutional responsibilities to students, faculty, staff, and other stakeholders through continued operations

Terminology and Scope

<table>
<thead>
<tr>
<th>Business Contingency Plan (BCP)</th>
<th>Disaster Recovery Plan (DRP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The all-encompassing plan that describes the processes and procedures put in place to ensure key functions can resume and be recovered should a disruption occur.</td>
<td>A disaster recovery plan is often limited in scope; such as an IT DR plan that deals with systems within a specific number of locations.</td>
</tr>
</tbody>
</table>

Why Business Continuity Planning?


BCP Opportunity ➔ Must Fix ➔ Recovery into BCP
What needs to take place ...
1. Recognize operational resiliency as an operational requirement
2. Assess Threats and Potential Impacts
3. Conduct a Business Impact Analysis (BIA)
4. Develop Solution Designs and Recovery Strategies
5. Develop Business Continuity Plans
6. Test and Exercise the BCPs, enhance Organizational Acceptance, and Training
7. Plan Maintenance

Planning Policy Statement
• Expresses executive commitment
• Demonstrates management support
• Highlights continuance of the institutional mission in the face of a crisis and the safety and protection of students, staff, and faculty.
• Outlines the goals, objectives, and measures of success
• Establishes policy and governance

Threat and Vulnerability Assessments
• Look inward and outward to identify and document potential threats
• Perform analysis to assess probability of occurrence and quantify the impacts
• Develop, implement, and test/execute remediation strategies
• Review and re-assess the threats and potential impacts periodically
• Continue to develop Rapid Response

Pick Low Hanging Fruit
• Walk your facilities
• Evaluate and report on campus life and safety issues
  – Develop and execute appropriate risk remediation strategies
• Enhance Rapid Response Capability
• T&VA Matrix and Analysis

Threats and Vulnerability Matrix

Do some analysis ...
• Rank order the events in likelihood of occurrence at your location
• Assess the probability of each event
• Assess value and quantify impacts using proven Risk Management practices and techniques
• Construct cost models
  – i.e., $R = P \times C \times T$
  
  $P =$ probability of event
  $C =$ cost of downtime
  $T =$ duration of event
Conduct a Business Impact Analysis (BIA):

- Talk to the business
  - Identify critical functions, processes, systems, staff, vital records, dependencies, and tolerances to business interruption or data loss
- Capture "Expected" Recovery Time Objectives"
- Conduct the gap analysis against ERTOS and recovery capability
- Vet ERTOS and drive to RTO
  - Don’t simply ask what they need … tell them what you will/can deliver
  - Distinguish between real or perceived wants vs. need

BIA Functional Requirements

- Applications/Network
- Vital Records
- Process Criticality Classification

Departments are broken down into processes which are ranked based on their criticality to the organization
Develop and Implement the Plans

- Develop, QC, sign off, and implement for key departments
- Extend scope and increase granularity
- Don’t forget the academic side too
- Prioritization of services and business functions against systems applying business tolerances and realistic and achievable Recovery Time Objectives

Basic BCP

- Plan owner(s) and person(s) responsible for individual plan components
- Activation trigger and activation sequences
- Contact lists (staff, agencies, vendors, …)
- Identification of critical processes and standard operating procedures
- Workaround procedures
- List of minimum resources required (staffing, space, technology, …)
- Vital records and alternate sources
- Pre-determined alternative location arrangements
- Incident log forms and work templates
- Document control (i.e., toolkit)

Testing, Organizational Acceptance, and Training

The purpose of testing is to achieve organizational acceptance that the business continuity solution satisfies the organization’s recovery requirements.

Plan Maintenance

Maintenance of a BCP process or manual is broken down into three periodic activities:
1. confirmation of information in the manuals and plans
2. testing and verification of manual and technical solutions established for recovery operations
3. testing and verification of documented organization recovery procedures.
Testing and verification of organization recovery procedures

As work processes change over time, the previously documented organizational recovery procedures may no longer be suitable.

Changes will be captured through a formalized CM process.

Maintain the Plans Summary

- Once the plans are written they are already obsolete
- Formalize Testing Plans
- Conduct Period Plan Reviews
- Incorporate changes as processes and technologies change
- Embed DR requirements in all purchase and implementation decisions

With that said ...

How is it Tulane, FARA, Hancock, Estes, Marriott, the Hard Rock Café, and OYO Geospace went from no plans or 'typical' plans to more robust preparedness plans?

Having been a victim ... victim no more!

What does it take?

- A recognition of need
- A willingness to do something about it
- A methodological approach to risk identification and mitigation
- Executive support
- Financial commitment
- Realistic goals and objectives
- Project Management

The first major mistake most make in developing a long term recovery plans is to place the responsibility squarely where it does not belong ... 

...in operations departments.

Contributions to failures

- 'Nah, ain't gonna happen to me' syndrome
- It's expensive
- It falls below the priority line
- It doesn't generate revenue
- It's seen as just an ongoing high cost
- It's natural for companies to do as little as they can get away with
- It's human nature to expect that we'll see this area underfunded
But not planning ... 

... can have dire consequences.

Thank You

Neal Sturm  
Vice President and CIO  
Fairleigh Dickinson University  
973-443-8689  
sturm@fdu.edu

Jim Lebo  
Assistant University Director of Computing Services and Project Management  
Fairleigh Dickinson University  
201-692-7139  
lebo@fdu.edu

Valuable Resources

• Insatiable Curiosity and Experience
• Common Sense
• Peers
• Professional Affiliations and Certifications
  – Disaster Recovery Institute International
• Government and Private Sector Agencies
  – National Institute of Standards and Technology
• Publications
  – Disaster Recovery Journal (www.drj.com)
• Consultants
• Search Engines
• Vendors

Top 11 Reasons Why Plans Fail

1. Lack of Commitment
2. Business and IT Are Not Linked
3. There Is No Working DR Plan
4. DR Plan Not Current
5. Not Correctly Testing the DR Plan
7. Lack of defined DR Roles and Responsibilities
8. Not Addressing the Right Risks
9. Unrecoverable backup data, lost vital records
10. Staff not being available to perform recovery
11. Cost and Gap