Contingency Planning: Disaster Recovery Strategies for Successful Educational Continuity

Adnan Omar
aomar@suno.edu

Igwe Udeh
iudeh@suno.edu
College of Business, Southern University at New Orleans
New Orleans, LA 70126, USA

Abstract

Disaster recovery plans (DRP) are becoming a key part of an organization's overall planning process because they ensure continuous availability of an organization's critical infrastructure at all times. A major component of these plans involves protecting business-critical data through backups and data replication. However, many organizations today have either inadequate DRPs in place or none at all. This is a major potential hazard because data is constantly threatened by hackers, viruses or natural disasters. The risk became catastrophically clear in 2005, when Hurricane Katrina devastated the Gulf Coast, impacting countless organizations. Companies with DRPs in place fared much better than those without such contingency plans. Thus, it is vital for every organization to have a DRP drafted, tested and implemented.

In the aftermath of Hurricane Katrina many universities have drafted and implemented DRPs. Many, however, still have not. This project focuses primarily on universities in the Gulf Coast area of the United States which suffered major losses of data due to Hurricane Katrina. The results are compared with that of Houston Community College (HCC) in Houston, TX, which proactively developed a sophisticated DRP post-Katrina, and used its DRP to recover rapidly from the ravages of Hurricane Ike in 2008. It is evident that DRPs are crucial for the protection of all universities. In fact, this study suggested a higher level of DRP awareness for all the universities that participated in this research as evidenced by a tremendous post-Katrina improvement in most of the eleven DRP assessment dimensions utilized in this research.

Keywords: Data loss, Natural Disaster, Disaster Recovery Plan, Backup, Educational Model.

1. INTRODUCTION

Regardless of geographical location, a workplace may be susceptible to events that cause physical damage. Floods and fires are often the most catastrophic events, but problems like hackers, viruses, and human errors also take an enormous toll. In light of recent events like Hurricane Katrina, many organizations, including universities and colleges, have begun to, or have been forced to think about how vulnerable they can be to natural disasters. Although such institutional vulnerabilities usually impact individual well-being, some mechanisms currently in place can help protect people and businesses, and most people are comfortable with these mechanisms. Unfortunately, not all organizations consider the impact of unexpected events on the workplace and the ap-

propriate response to emergent situations that have damaged or destroyed the workplace. A well-thought-out mechanism like a DRP can help to protect the organization's workplace and its crucial data during such times.

The objective of this project is to discuss the causes of data loss in general, effective backup strategies, recovery systems development, and their cost effects. The project intends to focus in particular on Information Technology (IT) department of some universities in the New Orleans and Houston areas which suffered major losses of data due to Hurricane Katrina.

Statement of the Problem:

At the heart of every organization are volumes of irreplaceable data that are updated daily. This information must be protected, secured through backups, and retrieved immediately, in the early phase of a disaster. All organizations must realize that future disasters are inevitable and preparation is essential to ensure that critical data is secured and easily retrievable. Implementing measures to minimize the potentially devastating effects of future data disasters is desirable.

Disasters such as system crashes, fires, hurricanes and earthquakes, often destroy an organization's electronic files and records, crippling its ability to recover rapidly. An appropriate DRP, including Data Backup and Storage, is necessary to retrieve the data in case of a disaster. However, not all organizations have a pre-planned DRP and a data backup and recovery system which would help at the time of data loss. Hence, all organizations should have a well prepared DRP as well as a cost-effective and reliable data backup system established to ensure the smooth functioning of an organization.

Since Hurricanes Katrina and Rita in 2005, contingency planning and risk management have taken very prominent positions in the planning process of residents and businesses in the disaster-prone Gulf Coast Region of the United States. This paper presents an overview of the pre-Katrina IT DRP practices as well as post-Katrina IT contingency plans developed and implemented by selected institutions of higher learning located along the Gulf Coast Region of the United States.

2. REVIEW OF LITERATURE

Although each key function of a manager – planning, organizing, commanding, coordinating, and controlling – originally identified by Henri Fayol (Fayol, 1930; Daft, 2008; Weaver, 2008) is important, it has been noted that effective planning and forecasting set the tone for successfully implementing the remaining functions (Navarro, 2009; Hambrick & Cannella, 1989). In fact, 80% of managers surveyed in a recent study indicated that planning is a very important part of their responsibility (Rigby, 2001). It has equally been suggested that the performance of a given organization is reflective of the ability of its managers to carry out each of the key functions, especially planning (Thompson, Purdy, & Summers, 2008; Neilson, Martin & Powers, 2008).

At the planning stage of the strategic management process, organizational leaders are expected to develop the mission, objectives, strategies, and policies for their enterprise (Leontiades, 1982). Furthermore, organizational plans fall into four broad categories: strategic, tactical, operational, and contingency. Strategic plans set the long-range goals that will guide the activities of the organization. Tactical plans identify the short-range goals that lower-level managers are tasked with completing. Operational plans are used to set work standards and schedules. Contingency plans, on the other hand, are used to minimize organizational risks by setting up alternative fall-back plans in case the original plans fall through (Pfinisgraff, 2009; Daft, 2008). Contingency plans prepare a company to appropriately respond to emergencies, setbacks, and unexpected situations, including loss of or limited access to key facilities, personnel, or proprietary data or information.

In today's IT-driven environment, data is vital for any organization; as such, no organization is immune from disasters such as disk crashes, power failures, human errors, and natural disasters that lead to loss of data. Data loss can be defined as "unforeseen loss of data or information" (Hoyles, 2007). This can have serious consequences on the day-to-day organizational functioning. Studies show that 44% of data loss is due to hardware or system malfunction; 32% is due to human errors; 14% is due to soft-

ware or program malfunction; 7% is due to virus infection, malware, spyware; and 3% is due to natural disaster as shown in Figure 1 (Solid Data Corporation, 2001).

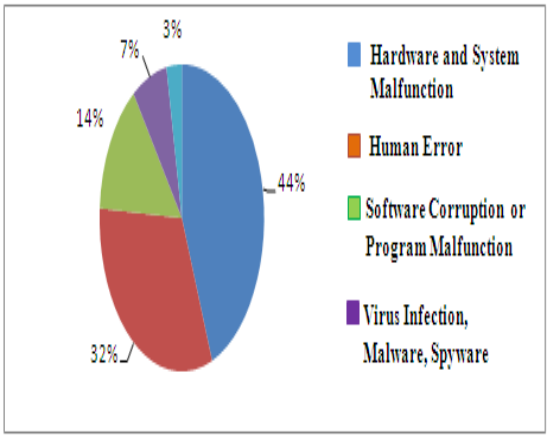

Figure 1: Causes of Data Loss

A commonly overlooked cause of data loss is a natural disaster. Although the probability of catastrophic natural disaster is small, the only way to recover from data loss due to a natural disaster is to store backup data in a separate location. As mentioned earlier, contingency plans prepare a company to appropriately respond to emergencies, setbacks, and unexpected situations, including loss of or limited access to key facilities, personnel, or proprietary data or information. Natural disasters may occur in the form of fire, flood, and lightning strikes followed by power surges.

A survey conducted by the Gartner Group, Contingency Planning and Strategic Research Group, and Price Waterhouse Coopers illustrates that 25% of all PC users suffer from data loss each year. Despite this, 96% of all business workstations do not backup their data. Approximately 70% of small firms experience a major data loss and go out of business every year, and an annual cost of $12 billion is spent on data loss recovery along with $55 billion computer virus damage to U.S. businesses (Remote Data Backup, 2004). These results make a strong case for the need for contingency planning in the form of sound Data Backup and effective DRP, as both of these elements sustain the life of an organization at the time of a disaster.

An essential element in contingency planning is a DRP which incorporates a sound Business Continuity Plan (BCP). The BCP consists of the precautions taken so that the effects of a disaster will be minimized, and the organization will be able to either maintain or quickly resume mission-critical functions (InfoSec, 2008). DRPs vary according to the needs, customers, and applications of each organization. A disaster recovery plan covers the hardware and software required to run critical applications, the data that an organization must maintain, and the steps necessary to maintain workforce continuity from remote locations (Cisco Systems, 2008).

Every organization must tailor its IT DRP to meet its requirements. IT DRP must be analyzed for its organizational processes and continuity needs, with a significant focus on disaster prevention. It is not uncommon for an organization to spend 25% of its IT budget on disaster recovery (Microsoft, 2008). An IT DRP must address three areas:

1. **Prevention** (pre-disaster): This area covers the pre-planning requirements – using mirrored servers for mission critical systems, maintaining hot sites, training disaster recovery personnel – used to minimize the overall impact of a disaster on systems and resources. This stage is critical because it helps organizations to maximize their ability to recover from a disaster (Chin, 2005).
2. **Continuity** (during a disaster): This is the process of maintaining core, mission-critical systems and resource "skeletons" (the bare minimum assets required to keep an organization in operational status) and/or initiating secondary hot sites during a disaster. Continuity measures prevent the whole organization from folding by preserving essential systems and resources (Chin, 2005).
3. **Recovery** (post-disaster): These are the steps required for the restoration of all systems and resources to full, normal operational status. Organizations can minimize recovery time by subscribing to quick-ship programs (Chin, 2005).

Figure 2 shows how an organization must plan its IT DRP/ BCP. Some important steps to follow in this process are: identifying the critical data within the organization; analyzing revenue and cost implications of a disaster recovery plan; framing a disaster recovery plan for all possible types of data loss; backing up data on a regular basis to a secondary source; replicating and/or storing a copy of critical data at an offsite location; testing the data protection and recovery procedures on a regular basis; and reviewing and updating the organization's continuity plan annually.

In 2006, a Computer World survey of small businesses with 1,499 employees or fewer indicated that 50% of these businesses had no DRPs, with 8% having no plan to set any DRP up (ComputerWorld, 2006). An organization's survival and recovery from a disaster, however, is dependent on a well structured DRP. This is as true for a business with 500 employees as it is for a university which may have as many employees and four to five times as many students, and must store important data such as student registration records, fee bills, attendance, payroll, courses, projects, inventory resources, etc.

Figure 2: Business Continuity Planning Lifecycle

Moreover, having a DRP itself is not sufficient; periodically testing the DRP is also mandatory. Although many organizations have a preset DRP, only a few of them check their DRPs regularly. In a poll conducted in 2004, 71% of the organizations admitted that they have not tested their DRPs in the previous year (Klien & Joseph, 2007).
While a natural disaster is the least likely cause of data loss, the magnitude of devastation is the highest and hence is of concern in areas that are prone to hurricanes and storms (Oskar, 2006). Thus, colleges, universities and other organizations in the Gulf Coast region of the United States require a well designed DRP and periodic data backup. Many colleges and universities in and around New Orleans which were the victims of Hurricane Katrina, for example, suffered severe data loss and, lacking a firm DRP, could not resume normal function immediately.

Hurricane Katrina, in 2005, forced the Gulf Coast residents to realize how unprepared they were for a massive disaster. The area's infrastructure was devastated, disrupting telephone communications and other elements essential to a modern economy. Thus, the storm highlighted a critical problem, especially in the colleges and universities, which lost vast amounts of critical data.

HCC Data Backup System

The database is the most important piece for ensuring little or no data loss to the remote database. In the main data center the production database is referred to as the primary production database and the production database in the remote data center is referred to as the secondary production database or standby database. This setup allows for multiple IT DR centers which can also have multiple remote production database copies. The DR data center is usually at a location that is considered safe.

HCC Remote DR Center

The HCC Data Center building was created to endure rain and wind. It is also equipped to cope with power outages. The remoter DR center that HCC uses is called CyrusOne. CyrusOne is a stand alone, single tenant building, that protects systems from many natural and man-made causes of outages. Each component of the CyrusOne datacenter is designed to ensure maximum availability in all conditions.

CyrusOne gives 100% protection or 100% compliance, specializing in the most cutting edge DR configurations and solutions. The hardware located at this datacenter duplicates the production hardware. To ensure

that performance is not compromised, the hardware in both datacenters should be identical.

HCC Data Replication

Replication is the copying of data from one system to another system. The end result is two consistent and equally workable data sets in multiple physical locations. The primary database is the online production database that is used for everyday business. The primary database is located in the main data center. The standby database is the offline production database used to duplicate production data and it is located at CyrusOne, the remote DR center (Figure 3). Oracle application Data Guard is used to help manage data replication. HCC has also created a manual management process for data replication. The process was designed using Oracle's Data Guard using log shipping. Log shipping allows high availability of the data to the remote site and limited loss of data. This method also allows recoveries to be performed independently of the database location, which means if the primary database crashes for any reason, the standby database can recover with the primary database being available. The recovery method is designed to allow for load balancing in all situations of a highly available database, during normal processing, takeover and online self-repair.

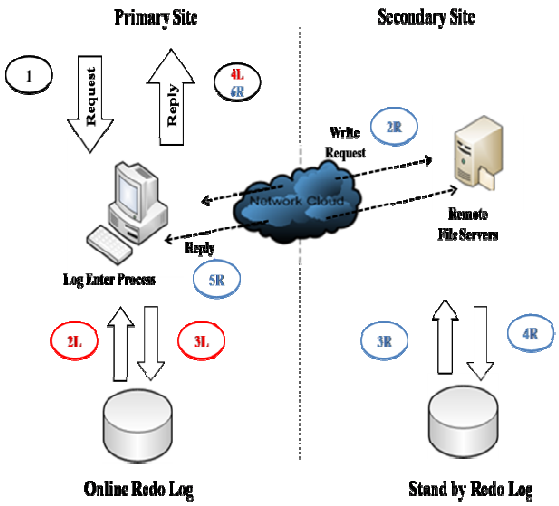

Figure 3: Data Guard Log Shipping

Oracle Log shipping occurs at the database level rather than the server level, which means that if something happens to the server it does not affect the database. One of the disadvantages of Oracle log shipping is that it is network dependent (Figure 3). As a result, there is some latency involved from the primary to standby database. The network infrastructure plays a major part in the speed and size of the logs being shipped. Because of the uncertainty of the network traffic, Data Guard is setup to ship the log files based on size and time of the last log shipped. What this means is that the log shipping parameter is set to ship logs when the log size reaches 20 kb or the time when the last switch was greater than 30 minutes. This also helps us control data loss. With these parameters being set in Data Guard, the management expectation of having only 30 minutes of data loss in the case of a disaster is being achieved. There are no built in failover capabilities for log shipping, which means that some downtime has to be incurred in the switch to the standby server. This also means that a maximum of 30 minutes of data loss may occur.

Testing the DRP is the key to ensuring its success. HCC has two system level testing dates per year to ensure that the data replication is accurate. The testing plan includes interrupting the production system and connecting to the remote data center. The network is re-routed to the remote site and all application is activated at the remote data center.

3. DATA COLLECTION

To assess the extent of risk management and contingency planning practiced by organizations located in an area with a running history of natural disaster, an eleven-point DRP instrument, based loosely on concepts from (Carruther, 2009) and (Beck, 2009) was developed and presented to IT managers of four institutions of higher learning located in the Gulf Coast region of the United States. The DRP instrument sought the pre- and post-Katrina answers to the following questions:

1. Is your hurricane preparedness plan satisfactory?
2. Did your plan achieve its aims?
3. Was your plan well tested and validated?
4. Was the content of your plan clear?

5. Are emergency contact numbers maintained?
6. Are there reliable offsite storage facilities?
7. Was the type of data storage employed economical?
8. What percentage of courses is offered online?
9. What percentage of course material is available on blackboard or other internet tools?
10. Was there a reliable backup?
11. Was there a data centre co-location?

Each IT manager was also requested to provide cost estimates for data backup and storage per annum for their university. The data collection procedure included completion of survey instruments; face-to-face interview with the IT managers; and review of official documents. All four surveyed institutions readily shared information with the researchers, within the limits allowed by their internal regulations. A simple weighted percentage computation was used to generate information on pre- and post-Katrina DRP trends in the surveyed institutions.

Data Analysis and Discussion

Table1 in the appendix shows survey responses of the IT directors of each university. Data from Table 1 was summarized into pre- and post-Katrina percentage positive response to allow for better trend analysis. Except for Questions 2, 7, and 10, Table 2 in the appendix shows a remarkable improvement in emergency preparedness between the pre-Katrina and post-Katrina IT directors' responses. In fact, there was a double or triple digit improvement in seven out of the eleven DRP survey areas.

Cost Estimates for Backup and DRP

Table 3 in the appendix shows the cost estimates for data backup of three universities. The reasons for the variations in costs are due to the backbone of infrastructure and the software being used by each university and their maintenance costs. Of the universities surveyed, HCC appeared to have the most comprehensive backup and DRP system. For approximately $576,000 HCC created one of the most reliable data backup and DRP system consisting of remote DR centers, data replication systems, and a sophisticated network that holds the system together as shown in Figure 3. A brief insight into the HCC system will illustrate this observation.

Furthermore, a comparison of information from Table 1 with information from Table 3 indicates varying trends in data backup and storage expenditure by the responding institutions. Although SUNO has fewer students than its counterparts, it spent proportionately more money on data backup and storage than the other respondents. However, SUNO also witnessed a 5000% growth (from 1% to 50%) in course materials available on blackboard or other internet tool and 833% growth (from 3% to 25%) in courses is offered online. This is a sharp contrast from the other institutions where the same variables remained flat pre- and post-Katrina. SUNO's IT DRP expenditures may be reflective of its acknowledgement of previous under-preparedness and a commitment to effective contingency planning going forward.

Proposed Model for Successful Educational Continuity

A model for successful contingency planning for an educational organization is presented in Figure 4. The model consists of ten steps. The first major decision in disaster planning is to acknowledge the possibility of a disaster. The Gulf Coast region will always be vulnerable to hurricanes (Blaisdell, 2006), so it is vital that all the colleges and universities prepare a contingency plan of their own to ensure that their business operations will not come to a halt. This encompasses a comprehensive, strategic approach to maintaining business operations while protecting the organization from a host of risks including hardware failure, viruses, theft, fire, and other natural disasters. The most common mistake is not planning for a potential disaster. Reasons for lack of preparation include the fear of cost or the belief that one's business is too small to be affected. The following steps are essential for successful DRP strategies:

Step 1-Goals and Objectives: Identify and analyze goals and objectives based on the needs of the organization, since disaster planning is not a one-size-fits-all concept. The primary objective of the plan should be to enable an organization to survive a disaster and to re-establish normal operations as early as possible.

Step 2-Backup Vision: Issues like prioritizing the type of data to be stored, the type of backup needed, and the time period of data storage must be considered. A secure storage location offsite must be chosen very carefully.

Step 3-Team Education: Educating the team members and key employees of the DRP is vital to mitigating the risks during a disaster. Every organization that is prone to disasters must use every available communication tool to drive home to each employee their DRP including tips to be followed during the event, instead of just posting the plan on the website.

Step 4-Implementation & Testing: Implement the DRP and validate the results obtained according to the needs of the organization and test the plan regularly under various conditions for its enhancement.

Figure 4: Model for Successful Educational Continuity

Step 5-Plan Upgrade: Upgrade the plan periodically to reflect organizational changes and technological advancements. Technology plays a vital role in any business where data is crucial. A proper platform must be created for businesses to keep up-to-date with the latest technology so as to remain compatible for safeguarding their data.

Step 6-Contact List Maintenance: Build solid contact lists of regular and key employees and update them regularly to establish a clear means of communication during a disaster.

Step 7-Blackboard Course Upload: For colleges and universities, the DRP must necessitate updating all course content, syllabi, student-faculty contact information on Blackboard each semester, whether they are taught online or not. This helps the faculty and students to continue their work while going through a disaster. Alternatively, an inexpensive piece of backup media such as a writable CD could mean the difference between business disaster and business survival. Depending on the amount of critical information one needs to protect, there is a wide array of affordable media available such as flash drive, floppy disk etc.

Step 8-Administration & Supervision: For educational institutions, the administration must ensure that faculties are uploading their course content on the Blackboard every semester and the material must be checked by the Blackboard administrator to make sure that the complete course requirement (syllabi, course material, schedule, faculty contact information etc.) are uploaded.

Step 9-Review & Repeat: Review, analyze, update, and repeat the entire processes (Steps 1 - 8) periodically, depending on the sensitivity of the data and the requirements of the organization.

Step 10-Test, test, and test: No plan is complete until it is tested. Testing helps adapt changes in the business and its technology infrastructure. In fact, testing is the only way to identify weaknesses in the plan and consequently address such weaknesses. Until the plan is tested, it cannot be considered usable.

The proposed Model for Successful Educational Continuity Planning (Figure 4) is similar to the existing Business Continuity Planning model (Figure 2) if the university offers all its courses online. A typical example of such institutions is the University of Phoenix and several new online academic institutions which have implemented extensive online-based curricula. However, most universities offer their courses through both traditional and online modes. This means that the Business Continuity Planning Model outlined in Figure 2 will not work well in this blended teaching environment. However the model proposed in Figure 4 will fit well into both teaching modes. With the Model for Successful Educational Continuity Planning (Figure 4) in place, traditional teaching has the

ability to utilize the internet as a repository for students to access the needed information uploaded on a suitable web platform, during emergency situations.

The rationale behind our proposed model (Figure 4) is that in case of disaster, university administrators will be able to immediately implement all traditional courses online to ensure educational continuity by providing students needed information without interruption. However, limitations for the proposed model (Figure 4) include the extra blackboard space required; the additional costs that accompany such increased capacity; and the total commitment of all members of the university community, especially the faculty, to implementing such a rapid shift from the traditional classroom to the e-learning environment.

Limitations of the Proposed Model for Successful Educational Continuity

All necessary technology for a viable DRP is readily available, and the cost of acquiring it is minimal in comparison with the annual institutional budget. However, in times of economic hardship, when institutions around the country are being adversely affected by the budgetary limitations of cash-starved governments, even a relatively minor fiscal commitment can be troublesome. While the ultimate responsibility for the achievement of DRP plan lies with the chief administrator of the university, there are a host of support personnel, including the E-learning leadership team, that are needed to monitor the overall implementation, and the DRP plan coordinator who will manage the day-to-day activities and serve as the liaison with the administration. Additionally, coordinators are needed to assist units in the planning and implementing sub-DRP. DRP is an expensive proposal because additional personnel are needed to perform functions that will include, but not limited to the following:

- Formulate teams to carry out each objective
- Monitor progress toward achievement of specific objectives
- Perform annual assessment of adherence to timeliness, and achievement of goals and objectives
- Assist with the modification of plans as needed
- Submit annual reports the status of the DRP

To insure continued involvement of the entire University community DRP teams will be assigned to carry out the activities of each sub-DRP including:

- Conducting appropriate activities for successful implementation of DRP
- Providing benchmark reports as appropriate
- Maintaining records of activities
- Identifying and communicate additional DRP needs
- Submitting progress reports to Plan Coordinator

4. CONCLUSION & RECOMMENDATIONS

Info-Tech's DRP in the Education Sector 2005 Benchmarking Report, shows that a surprising 47% of universities and colleges currently have no DRP in place. According to the report, however, these institutions acknowledge the importance of having such a plan. 68% of them say that they are currently in the process of planning and the 32% of schools with no DRP plan concede it may be up to three years before they have one in place. This may be because security and end-user support are higher IT priorities than disaster recovery. On the other hand, according to Info-Tech, among the 53% of schools currently with a plan in force, a whopping 86% are improving that plan (Schaffhauser, 2005).

A typical example of a successful implementation of the DRP Model for successful educational continuity, as outlined in Figure 4. With wind gusts approaching 100 mph, the 600-mile-wide category 2 Hurricane Ike hit Houston on the night of September 12, 2008. Although HCC was not much affected, predictably, the storm caused widespread power outage in the area, including at HCC. The power outage at HCC disrupted the college's primary data centre. However, HCC's system was equipped to cope with such a situation. The college immediately shifted the IP address of the primary data centre to the secondary data centre, and operations continued with minimum disruption. Experience from other universities offer many practical lessons for institutions that are subject to such catastrophic events.

Developing and implementing a well-organized DRP, using the model presented in Figure 4, will directly affect the recovery capabilities of a university. The extensive analysis of the DRPs of the four institutions has led to the conclusion that the Ten-Step model proposed here would best serve the long term IT contingency planning needs of any institution of higher education regardless of location.

REFERENCES

Beck, F. (2009). *Contingency Planning for Uncertain Times.* Retrieved July 30, 2009, from the World Wide Web: http://www.escsc.org/feo/feo.html

Blaisdell, M. (2006). *How Ready is Ready?* Retrieved June 15, 2008, from the World Wide Web: http://campustechnology.com/articles/41204/

Carruthers, M. (2009), *Emergency Planning and Coaching*, Retrieved July 30, 2009, from the World Wide Web: http://www.soulwork.net/emergency_plans.htm

Chin, P. (2005). *Introduction to Disaster Recovery Planning*. Retrieved June 17, 2008 from the World Wide Web: http://www.intranetjournal.com/articles/200503/ij_03_24_05a.html

Cisco Systems, (2008). *Planning for the Unexpected Disaster*. Retrieved August 16, 2008 from the World Wide Web: http://itresources.whatis.com/document;94621/tech-research.htm

Computerworld. (2006). *Protecting Critical Data in Small Organizations: Disaster Recovery, Business Continuity and Other Key Aspects of IT Strategy*. Retrieved July 8, 2008, from the World Wide Web: http://www.computerworlduk.com/whitepapers/index.cfm?whitepaperid=3605

Daft, R. (2008) *Management*, 8th ed. Mason, OH: Thomson South-Western Publishing Company.

Fayol, H. 1930. *General and Industrial Administration*. Translated from French by J. A. Coubrough. London, England: Pitman Publishing Ltd.

Hambrick, D.C., & Cannella, A.A. (1989) Strategy Implementation as Substance and Selling. *Academy of Management Executive, 3.* Pp 278-285

Hoyles, M. (2007). *Data Loss - The Scariest Term in Business Today.* Retrieved August 4, 2008, from the World Wide Web: http://www.articlestree.com/business/data-loss-the-scariest-term-in-business-today-tx486411.html

InfoSec. (2008). *Business Continuity Planning and Disaster Recovery Planning.* Retrieved July 3, 2008, from the World Wide Web: https://infosec.uga.edu/oldsite/bcpdrp/index.php

Klein, K. and Joseph, P. (2007). *Information Technology Disaster Planning: Lessons Learned from Katrina.* Retrieved June 13, 2008, from the World Wide Web: http://isedj.org/isecon/2007/3122/ISECON.2007.Klein.pdf

Leontiades, M. "The Confusing Words of Business Policy," Academy of Management Review 7 (1982): 45-48.

Microsoft. (2008). Data Protection and Disaster Recovery of Microsoft Windows Server 2008 and Microsoft Windows Vista Using HP Data Protector Express Software. Retrieved May 27, 2008, from the World Wide Web: http://whitepapers.techrepublic.com.com/abstract.aspx?docid=972363

Navarro,P. (Spring 2009). Recession-Proofing Your Organization,. *MIT Sloan Management Review 50,* 3; p. 45

Neilson,G., Martin,K., Powers,E. (June, 2008).The Secrets to Successful Strategy Execution *Harvard Business Review. 86*, 6; pg. 61.

Oskar, P. (2006). *Natural Disaster Causes 3% of Data Loss.* Retrieved May 23, 2008, from the World Wide Web: http://www.buzzle.com/editorials/9-4-2006-107556.asp

Pfinisgraff, M. (May 2009) Bolstering Your Risk Defense, M. *Risk Management 56,* 3 pp. 58 – 59

Rigby,D. (May 21, 2001). Don't Get Hammered by Management Fads. *The Wall Street Journal*, p. A22

Remote Data Backup. (2004). *Data Loss Facts & Figures.* Retrieved June 15, 2008, from the World Wide Web: http://74.125.45.104/search?q=cache:9_WiBls86eMJ:www.data_/restoration_services.com//What%2520is%2520Data%2520Loss.pdf+%2412+billion+is+spent+on+data+loss+along+with+%2455+billion+computer+virus+damage&hl=en&ct=clnk&cd=1&gl=us&client=firefox-a

Schaffhauser, D. (2005). *Disaster Recovery: The Time Is Now*. Retrieved June 17, 2008, from the World Wide Web: http://campustechnology.com/articles/40565_3/

Solid Data Corporation. (2001). Retrieved May 20, 2008, from the World Wide Web: https://secure.solidit.net.au/soliddata/signup.php?affiliate=222

Thompson,T., Purdy,*J.* & Summers,*D*.A. (Fall 2008) Five Factor Framework for Coaching Middle Managers. *Organization Development Journal*, *26.* pp. 63-72

Weaver, P. The Origins of Modern Project Management. PM World Today - March 2008 (Vol. X, Issue III). http://www.pmworldtoday.net;

Appendix

Table 1: Response of IT Directors to DRP Survey

Questions	Pre-Katrina				Post- Katrina			
	XAVIER	UNO	HCC	SUNO	XAVIER	UNO	HCC	SUNO
1. Is your hurricane preparedness plan satisfactory?	No	No	No	No	Yes	Yes	Yes	Yes
2. Did your plan achieve its aims?	No	No	Yes	No	Yes	Yes	Yes	No
3. Was your plan well tested and validated?	No	No	No	No	Yes	Yes	Yes	Yes
4. Was the content of your plan clear?	No	No	No	No	Yes	Yes	Yes	No
5. Are emergency contact numbers maintained?	No	Yes	No	Yes	Yes	Yes	Yes	Yes
6. Are there reliable offsite storage facilities?	No	No	Yes	No	Yes	Yes	Yes	No
7. Was the type of data storage employed economical?	Yes	Yes	No	Yes	Yes	Yes	Yes	No
8. What percentage of courses is offered online?	10%	20%	N/A	3%	10%	20%	N/A	25%
9. What percentage of course material is available on blackboard or other internet tool?	Optional	100%	N/A	1%	Optional	100%	N/A	50%
10. Was there a reliable backup?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
11. Was there a data centre co-location?	No	No	no	No	Yes, Colorado	Yes, Baton Rouge	Yes	No

Table 2: Summary of IT Directors Response to DRP Survey

Questions	Average Pre-Katrina Positive Response	Average Post-Katrina Positive Response	Average Post-Katrina DRP Improvement
1. Is your hurricane preparedness plan satisfactory?	0%	100%	+100%
2. Did your plan achieve its aims?	75%	75%	0%
3. Was your plan well tested and validated?	0%	100%	100%
4. Was the content of your plan clear?	0%	75%	+75%
5. Are emergency contact numbers maintained?	50%	100%	+50%
6. Are there reliable offsite storage?	50%	75%	+25%
7. Was the type of data storage employed economical?	75%	75%	0%
8. What percentage of courses is offered online?	8.25%	13.75%	+5.5%
9. What percentage of course material is available on blackboard or other internet tool?	25.25%	37.50%	+12.25%
10. Was there a reliable backup?	100%	100%	0%
11. Was there a data centre co-location?	0%	75%	+75%

Table 3: Cost Estimates for Data Backup and Storage per Annum for Selected Universities

Parameter	Xavier	UNO	HCC	SUNO
Backup Tapes	N/A*	$61,000	$15,000	$6,000
Offsite Data Storage	N/A*	$4,330	$5,000	$2300
Hardware maintenance	N/A*	$20,000	$6,000	$100,000
Software maintenance	N/A*	$21,600	$500,000	$200,000
Software Purchase for safeguarding the data	N/A*	$60,000	$50,000	$20,000
Number of employees and students the data storage can serve	N/A*	17,063	300,000	3,105
Total	N/A*	$166,930	$576,000	$328,300

*N/A = not available