I.J. Modern Education and Computer Science, **2014, 4, 57-67**
Published Online April 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2014.04.08

A Proposed Model for IT Disaster Recovery Plan

Hossam Abdel Rahman Mohamed
Computer & Information System Dept- SAMS, Maady Cairo
Hrahman@Transit.com.eg, Habdel@ENR.gov.eg

Abstract—IT disaster recovery planning is no longer an option. Reliable IT services have become an integral part of most business processes. To ensure the continued provision of information technology, firms must engage in IT disaster recovery planning. Surprisingly, there is little research on this topic. IT disaster recovery planning has not been fully conceptualized in mainstream IT research. A previously framework for assessing the degree of IT disaster recovery planning. Practitioners can use this study to guide IT disaster recovery planning. Our Disaster Recovery Plan is designed to ensure the continuation of vital business processes in the event that a disaster occurs. This plan will provide an effective solution that can be used to recover all vital business processes within the required time frame using vital records that are stored off-site. This Plan is just one of several plans that will provide procedures to handle emergency situations. These plans can be utilized individually but are designed to support one another. The first phase is a Functional Teams and Responsibilities the Crisis Management Plan. This phase allows the ability to handle high-level coordination activities surrounding any crisis situation. We will also discuss the development, finally maintenance and testing of the Disaster Recovery Plan.

Index Terms—IT Disaster Recovery, Datacenter Continuity, Risk Management, Recovery Strategy.

I. Introduction

Worldwide, businesses continually increase their dependence on IT systems for routine business processes. The business processes which directly rely on information systems and the supporting IT infrastructure often require high levels of availability and recovery in the case of an unplanned outage. As a result, the process of business continuity planning must intimately relate business processes to the traditional process of IT disaster recovery. [1]

Business continuity describes the processes and procedures an organization puts in place to ensure that essential functions can continue during and after a disaster. Business Continuity Planning seeks to prevent interruption of mission-critical services, and to re-establish full functioning as swiftly and smoothly as possible. [2]

A Disaster Recovery Management Datacenter can be defined as the on-going process of planning, developing, testing and implementing Disaster Recovery management procedures and processes to ensure the efficient and effective resumption of vital business functions in the event of an unscheduled interruption. With the growing dependence on I/S and the Business Process to support business growth and changes associated with their complexities, compounded with the complexities of changing technology, the following elements are key to implementing a comprehensive Disaster Recovery Program (Critical Application Assessment, Back-Up Procedures, Recovery Procedures, Implementation Procedures, Test Procedures, Plan Maintenance). [3]

An important part of preparing for a disaster understands the type of risks your organization faces. The top level of Table 1 lists some of the common IT failures that disrupt operations. The other risk types are grouped into malicious behavior, infrastructure related, and natural disaster categories. Nearly every organization in the world faces feasible risks from many if not most of these levels. [4]

Table 1: Type of Disaster

	Type of Disaster
A	Computer Failure, Corrupted ,Data, Labor Issues, Lost Data, Medical Emergencies, Network Failure, Software Errors
B	Bomb Threat, Bomb Blast, Biological Attack, Chemical, Spill/ Attack, Civil Unrest, Computer Virus, EMP, Espionage, Hacking, Human Error, Legal Issues, Logic Bomb, Sabotage, Theft, Terrorism, Workplace Violence
C	Blackouts, Brownouts, Burst Pipe, Environmental Hazards, Epidemic, Evacutation, Halon Discharge, HVAC Failure, WAN/ ISP Failure, Power Surge, Power Grid Failure, Sprinkler System Discharge, Transportation Disruptions
D	Earthquakes, Electrical Storms, Fire, Flooding, Hurricanes, Lighting, Tornadoes, Tsunami, Volcano, Wind Storm, Winter storms,

An effective disaster recovery plan ensures that you can quickly recover your data if it is lost. Be sure to develop and test your backup and restore strategies with appropriate resources and personnel.

A disaster recovery plan should ensure that all of your systems and data can be restored to normal operation quickly in the event of a natural disaster (such as a fire) or a technical disaster (such as a two-disk failure in a

redundant array of independent disks Level 5 (RAID-5) array). When you create a disaster recovery plan, you identify all of the actions that must occur in response to a catastrophic event. [5]

The paper will present in Section (2) IT disaster recovery planning and business continuity planning, Section (3) The Tiers of Disaster Recovery, Section (4) Demand for Comprehensive Disaster Recovery Planning, Section (4) Design Goals and finally proposed solution (Recovery Strategy Recovery Phases and Implementation and Evaluation).

II. IT DISASTER RECOVERY PLANNING AND BUSINESS CONTINUITY PLANNING

It appears that IT disaster recovery planning practices tend to lag behind contemporary trends in information technology. Even though modern enterprises have sophisticated information systems upon which they are utterly reliant, their IT disaster recovery plans may be limited to backing up data and devising methods for restoring data resources [6], [7]. Considering the integration of IT into all business functions and the reliance on technology, this view of ITDRP has become outdated [8]. Furthermore, rapid changes in business processes and organization structure necessitate a clarification of five points concerning IT disaster recovery planning:

First, although the terms "IT disaster recovery planning" and "business continuity planning" are occasionally used interchangeably, they are separate processes [9]. Business continuity plans are holistic strategies for keeping businesses operational following disaster [10], [11]. IT disaster recovery plans are aimed specifically at restarting IT services. In this role, they support business continuity plans [12]. The aims and objectives of IT disaster recovery plans should not conflict with those of business continuity plans.

The second point concerns the classification of incidents as IT disasters. IT disasters impact the organization in which the IT service is employed; including IT services which are outsourced to an independent vendor [13], [14]. If the vendor somehow fails to provide an ITservice, its clients may be faced with IT disaster [15]. IT disasters range from the accidental deletion of a file to a hurricane which destroys the building that houses the data center[16]. IT disasters may also stem from damage to supporting infrastructure in the area of the data center. These events cause damage to the inputs which collectively provide IT service. When the damage is such that it is no longer possible to provide an IT service, then an IT disaster is said to have occurred [17], [18].

Third, it should be noted that IT disaster recovery is for restoring IT services, but not necessarily restoring specific hardware and software architectures [19], [20], [21]. Examples of IT services include internet connectivity, telecommunications, and data storage and processing. IT services add value by providing additional capabilities to organizational members. The provision of such services relies on a combination of inputs from multiple resources, including hardware, software, data, human resources, and utilities[22]. Because these inputs may be destroyed in a disaster, it may not be possible or practical to return to pre-disaster conditions. Thus, disaster recovery for an IT service is complete when the service has been brought back online in a stable condition [23], [24].

Fourth, ITDRP does not involve the simplification or discontinuance of IT services [25], [26]. The purpose of ITDRP is not to simplify IT services so that they are easier to restore. Nor does it involve risk mitigation. While these are important functions, they are not part of ITDRP. Instead, the focus should be on devising alternatives means of restoring services following disaster [27].

Finally, since there are many interrelated IT services in an organization and there is a limited amount of resources to support these services, any action performed should be considered as continuous as opposed to discrete. Backups have long been viewed as a necessary part of ITDRP but backups are not discrete in that it is not an all or nothing condition. Backups can cover many parts of the systems but not all or they can be incremental and not cover instantaneous changes.

2.1.1 Benefits of a Datacenter Continuity/ Disaster Recovery Plan

- Allows your organization to avoid certain risks or mitigate the impact of unavoidable disasters by
- Minimizing potential economic loss
- Decreasing potential exposures
- Reducing the probability of occurrence
- Improving the ability to recover business operations
- Helps minimize disruption of mission critical functions – and recover operations quickly and successfully – in the event of a crisis by
- Reducing disruptions to operations
- Ensuring organizational stability
- Assists in identifying critical and sensitive systems
- Provides for a pre-planned recovery by minimizing decision making time
- Eliminates confusion and reduces the chance of human error due to stress reactions
- Protects your organization's assets and employees
- Minimizes potential legal liability
- Reduces reliance on certain key individuals and functions
- Provides training materials for new employees
- Reduces insurance premiums
- Satisfies regulatory requirements, if and where applicable

III. THE TIERS OF DISASTER RECOVERY

These tiers are summarized in Table 2

Table 2: Summary of Disaster Recovery tiers (SHARE)

Tier 0 - Do Nothing, No off-site data
Tier 1 - Offsite vaulting (PTAM)
Tier 2 - Offsite vaulting with a hotsite (PTAM + hot site)
Tier 3 - Electronic Vaulting
Tier 4 - Electronic vaulting to hotsite (active secondary site)
Tier 5 - Two-site two-phase commit
Tier 6 - Zero data loss

3.1 Tier 0 - Do nothing, no off-site data

Tier 0 is defined as a single site data center environment having no requirements to backup data or implements a Disaster Recovery Plan. On this tier, there is no saved information, no documentation, no backup hardware, and no contingency plan. There is therefore no DR capability at all. In our experience, some customers still reside in this tier. For example, while some customers actively make backups of their data, these backups are left onsite in the same computer room, or occasionally are not removed from the site due to lack of a rigorous vaulting procedure. A customer data center residing on this tier is exposed to a disaster from which they may never recover their business data (The typical length of recovery time in this instance is unpredictable. In many cases complete recovery of applications, systems, and data is never restored) [28]

3.2 Tier 1 - Offsite vaulting (PTAM)

A Tier 1 installation is defined as having a DRP, backs up and stores its data at an offsite storage facility and has determined some recovery requirements. The backups are being taken which are being stored at an offsite storage facility. This environment may also have established a backup platform, although it does not have a site at which to restore its data, nor the necessary hardware on which to restore the data, for example, compatible tape devices.

Recovery is dependent on when hardware can be supplied, or possibly when a building for the new infrastructure can be located and prepared. (The typical length of time for recovery is normally more than a week) [29]

3.3 Tier 2 - Offsite vaulting with a Hot site (PTAM + Hot site)

Tier 2 encompasses all requirements of Tier 1 (offsite vaulting and recovery planning) plus it includes a hot site. The hot site has sufficient hardware and a network infrastructure able to support the installation's critical processing requirements. Processing is considered critical if it must be supported on hardware existing at the time of the disaster. The backups are being taken and they are being stored at an offsite storage facility. There is also a hot site available and the backups can be transported there from the offsite storage facility in the event of a disaster. [30]

Tier 2 installations rely on a courier (PTAM) to get data to an offsite storage facility. In the event of a disaster, the data at the offsite storage facility is moved to the hot site and restored onto the backup hardware provided. Moving to a hot site increases the cost but reduces the recovery time significantly. The key to the hot site is that appropriate hardware to recover the data (for example, a compatible tape device) is present and operational.

(The typical length of time for recovery is normally more than a day) [31]

3.4 Tier 3 - Electronic vaulting

Tier 3 encompasses all the components of Tier 2 (offsite backups, disaster recovery plan, hot site) and, in addition, supports electronic vaulting of some subset of the critical data. Electronic vaulting consists of electronically transmitting and creating backups at a secure facility, moving business-critical data offsite faster and more frequently than traditional data backup processes allow. The receiving hardware must be physically separated from the primary site and the data stored for recovery should there be a disaster at the primary site. The backups are being taken and they are then being stored at an offsite storage facility. There is also a hot site available and the backups can be transported there from the offsite storage facility. There is also electronic vaulting of critical data occurring between the primary site and the hot site. [32]

The hot site is kept running permanently, thereby increasing the cost. As the critical data is already being stored at the hot site, the recovery time is once again significantly reduced. Often, the hot site is a second data center operated by the same firm or a Storage Service Provider. (The typical length of time for recovery is normally about one day) [33]

3.5 Tier 4 - Electronic vaulting to Hot site (active secondary site)

Tier 4 is defined as using two data centers with electronic vaulting between both sites and introduces the requirements of active management of the data being stored at the recovery site. This is managed by a processor at the recovery site and can support bi-directional recovery. The receiving hardware must be physically separated from the primary platform. The backups are being taken and they are being stored at an offsite storage facility. There is also a hot site available and the backups can be transported there from the offsite storage facility. There is also continuous transmission of data or connection between the primary site and the hot site, supported by high bandwidth connections.

In this scenario, the workload may be shared between the two sites. There is a continuous transmission of data between the two sites with copies of critical data available at both sites. Any other non-critical data still needs to be recovered from the offsite vault via courier in the event of a disaster. (The typical length of time for

recovery is usually up to one day) [34].

3.6 Tier 5 - Two-site, two-phase commit

Tier 5 encompasses all the requirements of Tier 4 (offsite backups, disaster recovery plan, electronic vaulting, and active secondary site), and in addition, will maintain selected data in image status (updates will be applied to both the local and the remote copies of the database within a single-commit scope). Tier 5 requires that both the primary and secondary platforms' data be updated before the update request is considered successful. The two sites are synchronized utilizing a high-bandwidth connection between the primary site and the hot site. [35]

Tier 5 also requires partially or fully dedicated hardware on the secondary platform with the ability to automatically transfer the workload over to the secondary platform. We now have a scenario where the data between the two sites is synchronized by remote two-phase commit. The critical data and applications are therefore present at both sites and only the in-flight data is lost during a disaster. With a minimum amount of data to recover and reconnection of the network to implement, recovery time is reduced significantly. (The typical length of time for recovery is usually less than 12 hours) [36]

3.7 Tier 6 - Zero data loss

Tier 6 encompasses zero loss of data and immediate and automatic transfer to the secondary platform. Data is considered lost if a transaction has commenced (for example, a user hits the Enter key to initiate an update), but the request has not been satisfied. Tier 6 is the ultimate level of Disaster Recovery. Local and remote copies of all data are updated and dual online storage is utilized with a full network switching capability. The two sites are fully synchronized utilizing a high-bandwidth connection between the primary site and the hot site. The two systems are advanced coupled, allowing an automated switchover from one site to the other when required. [37]

This is the most expensive Disaster Recovery solution as it requires coupling or clustering applications, additional hardware to support data replication, and high bandwidth connections over extended distances. However, it also offers the speediest recovery by far. (The typical length of time for recovery is normally a few minutes) [38]

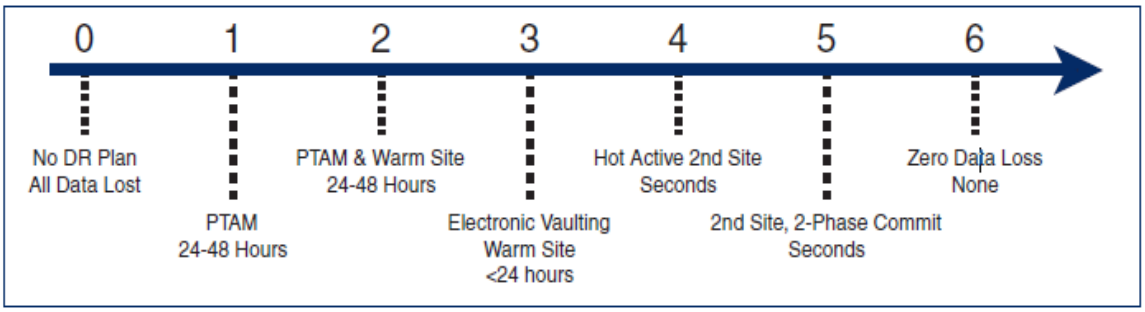

Fig 1 : The Typical length of Time for the Recovery in seven Tiers

IV. Demand for Comprehensive Disaster Recovery Planning

The process of Data center continuity planning must intimately relate business processes to the traditional process of IT disaster recovery.

4.1 Datacenter requirements for data recovery and availability

The organization governments are becoming increasingly accountable for how data is managed, protected, and secured. Policies and regulations vary from industry to industry, and the overall landscape of technical requirements continues to grow in complexity.

4.2 Increasing Availability Requirements

Overall, the increasing dependence on e-mail, electronic messaging, IP services, and cross platform governments applications is changing the way businesses use and rely on information systems. For many governments Organization, the use of e-mail has eclipsed that of voice for corporate communications, customer care, and vendor interactions. This dependency has created much more rigorous demands on operations to ensure availability of services and functional continuity plans.

In some cases, data corruption has brought entire corporate e-mail services to a halt due to two to three day recovery and rebuilds times. [39]

4.3 Storage growth trends

Year by year, storage requirements in enterprise operating environments continue to increase. Typical industry growth rates for disk storage range from 30% to 100% each year. [40]

The ubiquity of relational databases, e-mail systems, and rich media dependent systems (scanned documents, high-quality images, audio, video) all contribute to the growth of storage in data processing and customer environments. Emerging technologies (image recognition, advanced image analysis, wireless applications, smart

card, and so on) will only increase the demand for open, scalable, manageable, high performing, and relatively sophisticated storage systems.

4.4 Storage management challenges

Datacenter operating environments typically access large pooled arrays of disk and tape, which are managed by a central storage management application. Datacenter storage costs originally prevented decentralization and drove the need for highly efficient use of disk space. In addition to extensive use of tape for backup, these environments often also employ hierarchical storage management (HSM) applications, where infrequently used files are transferred to tape archives to free up disk space. A key aspect of mainframe environments which enables these approaches was the ability to logically partition (LPAR) an operating system environment. A logically partitioned system allows multiple instances of an operating system to essentially share locally connected hardware and network resources. [41]

4.5 Networking growth and availability

As storage management requirements increased along with data volume, many customers deployed locally attached storage management solutions and dedicated TCP/IP networks for backup/recovery operations in order to remedy TCP/IP bottle necking and congestion from backup operations. Today, Storage Area Network (SAN) technologies are being quickly adopted to enhance performance, scalability, and flexibility of shared storage resources. The SAN is a dedicated infrastructure for storage I/O, based on widely adopted industry standards for hardware components, Fiber Channel protocol (FCP), and ubiquitous SCSI standards. [42]

4.6 Capacity planning trend

Continuity of operations depends on having access to the data along with the ability to recover the data in the event of a disaster. [43] As storage consumption and growth continues, businesses depend more and more on accurate forecasting and capacity planning. Poor planning or lack of planning for storage often results in surprising halts to operations (unplanned outages), due to storage or network resource over consumption. Some platforms and technologies support dynamic expansion of resources, while others do not

V. Design goals

The principal goals of the Datacenter disaster recovery plan is to develop, test and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts Datacenter operations and information systems. The plan also documents the responsibilities, procedures, and checklists that will be used to manage and control the situation following an emergency or crisis occurrence. The Crisis Management Plan has been developed to accomplish the following objectives:

- Manage the Datacenter recovery operation in an organized and effective manner.
- The Datacenter Recovery Time Objective is the length of time a business can be without data processing availability and the Recovery Point Objective (RPO) is how old the data will be once the systems are recovered.
- Restore critical applications in Datacenter to the most current date available on backup tapes stored off-site. Updating the systems and databases will take place as the recovery effort progresses.
- Prepare Datacenter operation personnel to respond effectively in disaster recovery situations.
- Prepare Datacenter senior management personnel to respond effectively in a crisis situation.
- Limit the magnitude of any loss by minimizing the duration of a critical Datacenter application service interruption.
- Assess damage, repair the damage, and activate the repaired Datacenter.
- The need to ensure that Datacenter operational policies are adhered to within all planned activities
- Datacenter Disaster recovery capabilities as applicable to key customers, vendors and others
- Limit the magnitude or impact of any crisis situation to the various business units.
- The need to ensure that proposed contingency arrangements are cost-effective
- The need to consider implications on other company sites

VI. Proposed Solution

The disaster recovery solution that will be specifically addressed, within the scope of this plan, is the loss of access to the computer center and the data processing capabilities of those systems and the network connectivity. Although loss of access to the facility may be more probable, this Disaster Recovery Plan will only address recovery of the critical systems and essential communications. This scenario also assumes that all equipment in the computer room is not salvageable and that all critical telecommunications capability has been lost. In the event of a declared Disaster, key personnel will take immediate action to alert the Disaster Recovery Center. Restoration of the Critical Coverage will be provided after a Disaster is declared and after turnover of the disaster recovery backup site. It will include, without limitation, the following:

- Delivery of the Authorized User Data and Software archived in off-site storage to the Disaster Recovery Center
- Connecting Network lines to the Disaster Recovery Center

- Operating the Critical Applications on the Configuration at the Disaster Recovery Center
- Provide Critical Coverage at the Disaster Recovery Center
- Provide workspace and required equipment.

6.1 Recovery Strategy

The recovery strategy that will be discussed as part of this Disaster Recovery Plan will be to relocate critical Information Systems processing to an alternate computer-processing center. The processes will be recovered at the Disaster Recovery Services provider name and location of the Hot-Site. The Disaster Recovery Services provider name is responsible for ensuring that the system configurations and the associated network requirements are accurate and technically feasible at all times. Therefore, yearly testing will be a part of the alternate processing strategy Also; the associated network connectivity will be recovered, within the disaster recovery scenario, using the alternate processing strategy.

6.1.1 Recovery Phases

Datacenter Recovery activities will be conducted in a phased approach. The emphasis will be to recover the critical applications effectively and efficiently. Critical applications will be recovered over a period of time after data center activation.

Phase I

Functional Teams and Responsibilities, to Move the operations to the Disaster Recovery Backup Site and the Emergency Operations Datacenter, This activity will begin with activation of the Disaster Recovery Plan. There is a period of up to 24 hours allowed for organization and the turnover of the disaster recovery backup site.

Phase II

Disaster Recovery Action Plan, to recover critical business functions, restoration of the critical applications and critical network connectivity, the goal here is to recover the systems and network so that our customers can continue business.

Phase III

Evaluating and Testing the Disaster Recovery Plan, Return data processing activities to the primary facilities or another computer facility.

Table 3: Implementation Phases

Phase I *Functional Teams and Responsibilities*	**Phase II** *Disaster Recovery Action Plan*	**Phase III** *Evaluating and Testing the Disaster Recovery Plan*
• Damage Assessment Team • Disaster Recovery Team • Restoration Team • Operations Team • Customer Support Team • Major Plan Components - format and structure	• Backup and off-site storage procedures • Backup Facility • Disaster Preparation • Emergency Response • Recovery Procedures • Recovery Time Table	• Testing the Disaster Recovery Plan • Hot Site (DR Site) Test Procedures • Hot Site (DR Site) Test Planning • Application Testing Support • Post-Test Wrap-Up • Hot Site (DR Site) Test Schedule • Maintaining the Plan

6.2 Implementation and Evaluation’

6.2.1 Phase I

Functional Teams and Responsibilities

6.2.1.1 Damage Assessment Team

The Damage Assessment Team assesses the extent of the damage to the Data Center, reports to the Executive Team, and makes a recommendation on declaring a disaster. The major pre-disaster responsibility is to determine appropriate considerations/criteria for identifying the extent of the damage and the estimated duration of the outage. The disaster responsibilities and actions are:

- Receive the first alert regarding the disaster.
- Ensure that the NIH police/fire departments have been notified.
- Coordinate with the police and/or fire department to provide for safety, security, and access to the damaged facility.
- Notify the DCSS Director or alternate regarding the potential disaster.
- Assess the damage to each area of the computer facility.
- Brief the Director or alternate, communicating the recommendation(s).

6.2.1.2 Restoration Team

The Restoration Team brings the hot site systems to operational mode by managing the relocation of services to the hot site, initiating and managing the recovery procedures at the hot site, and responding to operational problems at the hot site. The Restoration Team also manages the relocation of services back to the Data Center.

The pre-disaster responsibilities are:

- Establish and maintain the recovery procedures for the hot site systems.
- Manage and maintain the backup procedures.
- Establish and maintain the disaster recovery data communications link.
- Plan and conduct regular hot site tests.

The disaster responsibilities and actions are:

- Coordinate recovery procedures with hot site personnel.
- Restore the operating systems environments on the hot site host systems.
- Establish the data communications link to the hot site.
- Verify the operating systems and all other system and communication software are working properly.
- Restore the application files.
- Support the operations at the hot site by resolving problems and monitoring and maintaining the data communications link to the hot site.
- Manage the backup tapes that were sent to the hot site.
- Ensure all required backups of the entire system are completed in preparation for leaving the hot site.

6.2.1.3 Operation Team

The Operations Team assists in the recovery operations and manages the operations of the computer systems at the hot site.

The pre-disaster responsibilities are:

- Ensure that appropriate backups are made on the prescribed, rotating basis and are ready to be taken off-site.
- Maintain current, up-to-date systems operations documentation, ensuring that this documentation is suitably stored off-site.

The disaster responsibilities and actions are:

- Provide assistance to the Restoration Team in the restoration of the system software and customer files, as required.
- Run system and operation jobs, as required.
- Implement and maintain a problem log.
- Provide information to the Customer Support Team regarding the status of the system, operations, and the customer jobs.
- Effect the transfer of media and print output from the hot site to suitable customer pickup location(s).
- Coordinate the shutdown of the hot site operations and the transfer back to the Data Center.

6.2.1.4 Customer Support Team

The Customer Support team provides assistance to customers during the disaster from the time the disaster is declared until operations resume at the Data Center.

The pre-disaster responsibilities are:

- Advise and consult with application customers regarding their disaster recovery requirements.
- Assist application customers during disaster recovery tests.

The disaster responsibilities and actions are:

- Notify participating application customers that a disaster has been declared.
- Advise customers of the disaster recovery system status, availability, and accessibility.
- Provide problem diagnosis and resolution guidance/assistance to application owners and their customers.

6.2.1.5 Disaster Recovery Team

The Disaster Recovery Team has been organized to assess the damage to the computer facility, to control and coordinate recovery/backup actions, and to make recommendations to the Director of Information Services. The team will consist of a cross section of persons responsible for one or more of the following functions:

- Systems software
- Application software
- Communications
- Operations
- Facilities
- Hardware

The team's responsibilities include:

- The team will be contacted and assembled
- Establish facilities for an emergency level of service within 2.0 business hours.
- Coordinate activities with disaster recovery team, first responders, etc.
- Report to the emergency response team.

6.2.1.6 Major Plan Components - format and structure

Members of the management team will keep a hard copy of the names and contact numbers of each employee in their departments. In addition, management team members will have a hard copy of the company's disaster recovery and business continuity plans on file in their homes in the event that the headquarters building is inaccessible, unusable, or destroyed. If a manager or staff member designated to contact other staff members is unavailable or incapacitated, the designated backup staff member will perform notification duties.

6.2.2 Phase II

Disaster Recovery Action Plan

6.2.2.1 Backup and off-site storage procedures

All disks are dumped to tape on weekly cycles. The

latter set of tapes are referred to as the off-site backup tapes. Both backups are cycled through six sets of tapes so that six successive weeks worth of backups are always maintained.

a) Backup strategy

- The Information Services tape library contains all the required tape sets for the weekly Differential Backups. There are 5 backup sets, WEEK1, WEEK2, WEEK3, WEEK4, and LAST with 12 tapes per set. This device is a Dell LTO4 Tape Library that is downward compatible to the LTO2 tapes
- Offsite Backup tapes are rotated on a four (4) week cycle.
- All Offsite Backup tapes are stored at the data storage facility.

b) Backup tape sets

- Differential Backups - Contains system data files changed since the last Full Backup
- Full Backups - Contains all system data files maintained in the Data Center
- Offsite Backups – Full Backup for Offsite storage
- Semi-Annual Backups - Another Full Backup twice a year in June and December

c) Backup tape schedule

- Differential Backups - Scheduled Sunday – Thursday nights
- Full Backups - Scheduled Friday nights
- Offsite Backups - Scheduled Saturday nights
- Semi-Annual Backup 1-– December
- Semi-Annual Backup 2 – June

d) Backup software and media rotation [44]

- Symantec Backup Exec version 12 is used to backup the servers. The software has been very effective in backing up data and restoring lost data and it is upgraded by the Information Services staff when new updates are made available.
- Sunday starts the new backup week and the tapes will be rotated automatically using job policies for each server within the Backup Exec software.
- The Offsite containers are delivered every Thursday to the Information Services Helpdesk and inserted into the tape library for the upcoming cycle. The tapes are removed every Monday morning and retrieved that same afternoon for offsite storage.
- Symantec Net Backup is used to backup hard drive information (Desktop, My Documents, Favorites) on faculty and staff desktop computers to the SAN backup share drive. This drive is part of the nightly Backup Exec backups, but the user must run the Symantec Net Backup application because it does not run automatically.

6.2.2.2 Disaster Preparation

This section outlines the minimum steps needed in order to ensure the District can fully recover from a disaster.

- The disaster plan must be kept current and all personnel on the recovery team must be made aware of any plan changes and fully trained to perform their assigned tasks.
- The offsite storage area should be inspected annually to ensure it is clean, organized and that the correct backups are in storage.
- The fire fighting system in the computer room should be inspected annually. Department heads should be aware of the consequences of a disaster and develop alternate data processing procedures while recovery is in progress.
- The Facilities department maintains and distributes the District's Emergency Telephone Numbers List of pertinent personnel to contact in case of an emergency.
- Procedures and lead times for replacement equipment and communications should be established.
- All computing personnel should be informed of the proper emergency and evacuation procedures.

6.2.2.3 Emergency Response

This section details the basic actions that need to be taken in the event of a disaster situation.

- The Director of Information Services or designee should be notified as soon as possible.
- The disaster recovery team should be notified and assembled as soon as reasonable under the circumstances.
- Team members should assess damages to their individual areas of expertise. The recovery procedures should include an estimated timeline for restoration of specific services based on the service priority. The estimate can include alternative interim solutions for specific services during the reconstruction of permanent solutions.
- Team members should advise the Director of Information Services as to the extent of damage and recovery procedures necessary so that the decision to move the Data Center can be made after the assessment of the damage to the current facility has been determined.
- Pertinent vendors should be contacted and negotiations should be made for the delivery of equipment, delivery time should be noted. All department heads should be informed of the decision and given an estimated time for the return to either full or degraded services.
- Each member of the disaster recovery team should supervise his or her own area of expertise.
- The computer facility should be secured.

6.2.2.4 Recovery Procedures

Recovery from a complete failure to a degraded mode of services may be necessary. In this case it may be possible to bring up individual departments on a priority basis.

- The decision to operate in a degraded mode and the order in which departments are to be brought back into service should be made by the Director of Information Services in consultation with team members and the Vice President, Finance and Administrative Services.
- An inventory of the status of existing equipment and files should be compiled.
- The Director of Information Services should coordinate the move of facility.
- Vendors should be contacted to initiate delivery of replacement equipment to the Escondido Center backup facility. The estimated time of delivery should be noted.
- A new offsite (backup) storage facility should be located and used immediately, if necessary.
- All facility systems should be verified operational at this time.
- Systems should be tested and loaded as soon as the vendors release them to the District.
- Communications, networking, operations and applications software personnel should be prepared to install and or setup their individual function in the appropriate order.
- All department heads should be made aware of progress and or setbacks on a regular basis.
- Existing safety and emergency procedures at the backup facility should be examined for their adequacy as a computer room.

6.2.2.5 Recovery Time Table

The following timetable is estimated and does not take into account the amount of time required to input data held on hardcopy during the recovery period, or re-inputting data which may have been lost during recovery.

Day 1 Convene the disaster recovery team, ascertain the extent of the damage and evaluate potential consequences, notify department heads, contact vendors, discuss options.

Day 2-4 Release formal communication to the campus community. At the disaster site, carry-out a safety inspection, inventory status of existing equipment and files, make a full evaluation of the damage, provide detailed accounting for insurance claims, and retrieve vital documents and reusable equipment.

Day 5-12 Obtain system data backup tapes and ensure all relevant documentation is retrieved from the offsite storage facility for restoration of network services and information systems. Take delivery and install new equipment. Restore programs and data, and test integrity of programs and data. Reconfigure communications network equipment and ensure that the reinstated communications environment is operable and tested. Make priority determination of data processing and systems, restore partial operation to priority departments, and enforce current computer and information systems security standards.

Day 13-14 Before undertaking any processing transfer security copies of all files and programs to offsite storage location. Restore full communications and networking capabilities. Work with departments to verify data and operation of application. Start processing in accordance with prepared production schedules.

6.2.3 Phase III

Evaluating and Testing the Disaster Recovery Plan

6.2.3.1 Testing the Disaster Recovery Plan

Testing and exercising the Disaster Recovery Plan helps to verify that the recovery procedures work as intended and that the supporting documentation is accurate and current. Testing also provides an opportunity to identify any omissions in recovery procedures or documentation and to determine whether personnel are adequately prepared to perform their assigned duties. Therefore, Division of Computer System Services (DCSS) regularly schedules exercises of its Disaster Recovery Plan at the vendor hot site, referred to as hot site tests (DR Site).

6.2.3.2 Hot Site (DR Site) Test Procedures

DCSS schedules the hot site tests for a two day period, covering the disaster recovery procedures. The first day is dedicated to exercising the system recovery procedures and establishing the communications link. The second day is dedicated to testing the recovery of participating applications. The hot site tests are managed and conducted by members of the Restoration Team, the Operations Team, and the Customer Support Team, referred to collectively as the HST Team.

Prior to the HSTs, the HST Team determines which backup tapes will be used for the tests, establishes a test plan which outlines the goals and activities for the given HST, conducts the necessary preparations for the test, and assists customers in their preparations for the HST. During the tests, in addition to providing customer assistance, the HST Team participants maintain a running log of the test activities to assist in the post-test review.

After every test, the HST Team participants meet to discuss the tests in order to improve the recovery procedures and the plan documentation. The HST Team also schedules a meeting with the customers to gain their input and suggestions for improvements.

6.2.3.3 Hot Site (DR Site) Test Planning

To ensure a successful hot site test, the HST team will:

- Confirm with the hot site vendor that the hot site mainframe, Unix computer, and data communications configurations will meet the HST

needs, and that the hot site will be ready for the test. (Two to three months prior to the scheduled test)
- Set the objectives for the test and establish action items for the team in preparation for the test. (At least two months prior to the scheduled test)
- Disseminate information to the user community regarding the test. (Six to eight weeks prior to the scheduled test)
- Confirm that preparatory tasks are being completed and review the schedule of events for the days of the HST. (Four to six weeks prior to the scheduled test)
- Discuss the final test preparations with the hot site vendor to confirm the hot site configurations, to obtain the information required for the mainframe backups, and to reconfirm the hot site will be ready. (Two to three days before the scheduled backups for the test will be taken)
- Send the backup tapes and tape lists to the hot site. (One week prior to the scheduled test)

6.2.3.4 Application Testing Support

The HST Team offers user support during a hot site test to assist the application owners/participants in successfully running their applications at the alternate site. The assistance includes help with test preparations, on-call support during the duration of the test, resolving reported problems, and serving as the liaison between the user and the HST Team.

Test preparation support includes:

- Ensuring the users have made all appropriate preparations for their data to be available for the HST,
- Ensuring the users are ready for the HST and have no further questions, and
- Ensuring users have the necessary contact phone numbers for user support during the HST.

Hot site test support includes:

- Notifying those users who have not logged on that the disaster system is up and ready for user testing,
- Responding to general user questions and to user problem reports, ensuring they are resolved, and
- Recording all problem reports and general notes to a system status database that is made available to users to read.

6.2.3.5 Post-Test Wrap-Up

Two debriefings are schedule on the days immediately following the hot site test. One is for the HST Team participants to assess the systems software recovery procedures. The second is for the user community who participated in the HST.

These meetings are general discussions to address:

- Areas where the exercise was successful,
- Problems that were encountered, and
- Suggestions for improvements.

Based on the conclusions, an "action list" of improvements to be made prior to the next test is developed and responsibility for implementing them is assigned.

6.2.3.6 Hot Site (DR Site) Test Schedule

The HST Team will have access to the systems on every quarter bear year, to restore the system/subsystem software and test the data communication link prior to the application users' access on the following day.

6.2.3.7 Maintaining the Plan

The Disaster Recovery Coordinator of the Data Center is responsible for the maintenance of this document. The plan is updated as needed:

- In response to events such as office moves, telephone number changes, new personnel joining DCSS, retirements, duty changes, and additions or deletions of participating applications;
- After each hot site test to reflect the recommendations resulting from the post-test wrap-up debriefings; and
- After a periodic review of the plan.
- As sections of the plan are updated, the revised sections are posted to the internal DCSS web site to ensure the most current information is available to DR team members. DR participants are notified of the changes and are encouraged to produce printouts for their copies of the disaster recovery plan.
- Additionally, the plan will be updated in the event an actual disaster occurs. The plan will be reviewed and updated at a convenient point after the initial responses to the disaster have been completed.

VII. Conclusion

This research delivers three important contributions. First, it draws attentions to the serious underrepresentation of IT disaster recovery planning research in the IT field. Second, it provides a basis for conducting work in this area by framing the concept of IT disaster recover planning and conceptualizing a definition grounded in practitioner literature. Finally, it provides a rigorously developed measure of ITDRP; these efforts provide an initial first step toward a better understanding of the complexities of IT disaster recovery planning.

References

[1] Anderson, J. "New trends in backup: Is your disaster recovery plan keeping up?" *The eSecurity Advisor*, 8, 2, 2008, pp. 58.

[2] Pregmon, M. "IT disaster recovery planning: Are you up and ready? Part 1: Risk analysis," Journal of the Quality Assurance Institute, Volume 27, Number 2, 2007, pp. 23-24.

[3] Kweku-Muata, Harvey Millarb, Anito Josephc / Using formal MS/OR modeling to support disaster recovery

planning, European Journal of Operational Research ,Volume 141, Issue 3, 16 September 2002, Pages 679–688
[4] Bell, Judy. "Why Some Recovery Plans Won't Work." Disaster Recovery Journal. Spring 2003: 30 - 32.
[5] Hoban, Frances; Kerkin, Kate1/ Disaster Recovery - Planning Challenges, Planning News, Volume 35 Issue 8 (Sept 2009)
[6] Jackson, R. "In times of crisis," Internal Auditor, Volume 31, Number 4, 2008, pp. 46-51.
[7] Preimesberger, C. "On the brink of disaster," eWeek, Volume 11, Number 2, 2008, pp. 31-38.
[8] Hayes, J. "Reaping the whirlwind," IEE Review, Volume 13, Number 3, 2005, pp. 29.
[9] Harney, "Business continuity and disaster recovery: Backup or shutdown," eDoc Magazine, Volume 3, Number 3, 2004, pp. 42-43.
[10] Brodkin, J. "When one data center is not enough," Network World, Volume 25, Number 5, 2008, pp. 32.
[11] Crowe, M. "Today's disaster recovery: A holistic approach to remediation," Illinois Banker, 43, Number 12, 2007, pp. 16-17.
[12] Connor, D. "Users assess plans for data protection, disaster recovery," Network World, Volume 22, Number 10, 2005, pp. 10.
[13] Curtis, G. "Beyond disaster recovery," Directorship, Volume 23, Number 2, 2008, pp. 38-42.
[14] Lewis B., Templeton, G., Byrd, T. "A methodology for construct development in MIS research." European Journal of Information Systems, Volume 14, Number 2, 2005, pp. 388-400.
[15] Havenstein, H., Fisher, S., Thibodeau, P. "IT execs race against time along Gulf coast," Computer World, Volume 40, Number 6, 2006, pp. 7.
[16] Saccomanno, P., Mangialardi, V. "Be prepared for IT disasters," Canadian Consulting Engineer, Volume 32, Number 4, 2008, pp. 35-40.
[17] Gold, L. "Security still tops tech concerns," Accounting Today, Volume 22, Number 3, 2008, pp. 25-28.
[18] Lohrman, D. "Disaster Recovery: A process – not a destination," Public CIO, Volume 8, Number 2, 2007, pp. 54.
[19] Rolich, P. "Setting priorities: Business continuity from an IT perspective – is it better to be right or liked?" Tech Decisions, Volume 9, Number 2, 2008, pp. 11-14.
[20] Hall, M. "On the Mark," Computer World, Volume 21, Number 11, 2007, pp. 20.
[21] Mearian L. "Key financial firms compare notes on disaster recovery," Computer World, Volume 38, Number 31, 2004, pp. 43.
[22] Lanter, A. "Staying ahead of the disaster recovery plan: Requirements are changing at record speeds," Illinois Banker, 44, Number 4, 2008, pp. 6-8.
[23] Rolich, P. "Setting priorities: Business continuity from an IT perspective – is it better to be right or liked?" Tech Decisions, Volume 9, Number 2, 2008, pp. 11-14.
[24] Hall, M. "On the Mark," Computer World, Volume 21, Number 11, 2007, pp. 20.
[25] McLaughlin, L. "Rethinking disaster recovery," CIO, Volume 21, Number 6, 2008, pp. 23-26.
[26] Gagnon, R. "When disasters strike," Mass Builder, Volume 25, Number 3, 2008, pp. 21-22.
[27] Guster, D. McCann, B., Krzenski, K., Lee, O. "A cost effective, safe, and simple method to provide a disaster recovery plan to small and medium businesses," Review of Business Research, Volume 8, Number 4, 2008, pp. 63 71.
[28] Byrd, T., Turner, D. "Measuring the flexibility of information technology infrastructure: exploratory analysis of a construct," Journal of Management Information Systems, Volume 17, Number 1, 2000, pp. 167-208.
[29] Green, R. "Peace of mind: Disaster recovery plans can keep your business alive," California CPA, Volume 33, Number 2, 2005, pp. 23-24.
[30] Landa, H. "Planning for disaster," Associations Now, Volume 11, Number 3, 2008, pp. 21-22.
[31] Bradbury, C. "Disaster! Creating and testing an effective recovery plan," British Journal of Administrative Management, Volume 23, Number 4, 2008, pp. 14-16.
[32] Hurdis, B. "Disaster recovery and business continuity planning: A strategic investment," Illinois Banker, Volume 44, Number 3, 2008, pp. 10-11.
[33] Mearian, L. "Hurricane, floods, put IT staff to the test," Computer World, Volume 39, Number 36, 2005, pp. 4.
[34] Mearian, L. "IT execs must fight for disaster recovery money," Computer World, Volume 39, Number 35, 2005, pp. 19.
[35] Pabrai, U. "Contingency planning and disaster recovery," Certification Magazine, Volume 5, Number 8, 2004, pp. 38-39.
[36] Pregmon, M. "IT disaster recovery planning: Are you up and ready? Part 2: Internal Control," Journal of the Quality Assurance Institute, Volume 27, Number 3, 2007, pp. 25-28.
[37] Beaman, B. and Albin, B. "Steps to disaster recovery planning," Network World, Volume 25, 6, 2008, 25.
[38] Fallara, P/ Disaster recovery planning , Potentials, IEEE Journals , Volume: 22 , Issue: 5 ,Jan. 2004
[39] Budko, R. "Messaging disaster recovery – A necessity for disaster recovery," Government Procurement, Volume 14, Number 10, 2007, pp. 30-31.
[40] Vijayan, J. "Data security risks missing from disaster recovery plans," Computer World, Volume 39, Number 41, 2005, pp. 16-18.
[41] Kumar, R., Park, S., Subramaniam, C. "Understanding the value of countermeasure portfolios in information system security," Journal of Management Information Systems, Volume 25, Number 2, 2008, pp. 241-279.
[42] Mearian, L. "Users are rethinking disaster recovery plans," Computer World, Volume 39, Number 36, 2005, pp. 8.
[43] Postal, A. "Disaster recovery plan seen as critical to GEB's survival," National Underwriter, Volume 35, Number 4, 2007, pp. 23-25.
[44] Symantec, "State of the data center regional data – Global," Second annual report, Cupertino, CA, 2008.

Hossam Abdel Rahman Mohamed: Master of computer science & information system - Sadat Academy - Dept Computer and Information System ,Maady , Cairo , Egypt - He is currently position Data Center Operation Team leader at Trans IT Company - Ministry of Transportation