IT Disaster Recovery Plan for "X" Company

Enrique Fernández
Computer Science
Juan Ramírez, Ph.D.
Electrical & Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

Abstract *— The Company "X" is a small business with 25 employees located in Old San Juan area, specifically in the "Z" building; the company is dedicated to providing retirement plan services and administration thereof. It is currently expanding in the areas of Miami, Florida and Mexico City, Mexico. As a result of this expansion plan an internal look is mandatory and as part of this introspection a Disaster Recovery Plan or DRP is very important in the overall plan for business continuity. Presently, the company has a local area network with dozens of interconnected stations that use the Internet intensively, which requires it to establish a configuration in terms of routing, control, security and diversity of services with a high degree of traffic processing.*

Key Terms *— Disaster Recovery Plan, Information Technology, Potential Disruptive Threats, Retirement Plan Services.*

PROBLEM STATEMENT

Each year, millions of businesses are affected by floods, earthquakes, fires, tornadoes, vandalism, theft, hurricanes, terrorist acts, etc. Businesses that survive these incidents are those which are prepared for these events, having previously estimated the potential damage that may occur to these events and implementing the controls necessary to prevent or reduce them.

The company is a private entity with legal personality, administrative and patrimonial autonomy.

OBJECTIVE

Prepare the Disaster Recovery Plan for "X" Company and propose changes to safeguard the resources, processes and information.

Specific Objectives

We will pursue the following specific objectives, which will help us define the scope of our objective:

- Identify the DRP functionality, the necessary staff, operating locations, alternative equipment, settings to be used, documentation guidelines and procedures.
- Identify potential causes of the organization activities disruption.
- Introduce the DRP to be produced before it affects the resources availability and business processes as may be produced by a disaster.
- Identify actions that the company should maintain so that the continuity plan is in effect permanently.

JUSTIFICATION

The DRP are detailed procedures to facilitate recovery of the operational capabilities of a company. Therefore, the expansion plans into other market require business continuity. It can only be achieved if you include all the elements that can affect the supply of services. The necessary actions are taken to minimize and resolve any type of disaster.

SCOPE AND FEASIBILITY

This proposal or model to guide the company after disaster strikes either natural or induced.

METHODOLOGY

The method used is the deductive method which is a method of reasoning used in research where specific applications and / or consequences follow from general principles or postulates.

Techniques and Instruments

Techniques and instruments are the tools for the collection of data on the reality that this inquiring:

- Field Design: Data collected directly by the researcher considered primary.
- Survey: Employee Survey.
- Observation: Communication structure, hardware and software.

Data Analysis

Through statistical technique, tabular and graph data has been processed for a better understanding so we can deduce Conclusions, Recommendations and Proposal.

- Is the company is protected in a disaster?
  100% of respondents said no and that having Plan disaster recovery, the company would be protected.
- Do you know of a disaster recovery plan?
  100% say that they are unaware of the existence of the recovery plan.
- Do you know how to operate the disaster recovery plan?
  15% Yes 85% No; 15% indicates that the operation of the DRP know, because in previous works they were exposed, 85%; 17 respondents did not know the operation.
- Do you know if the company has standards, security policies and procedures?
  40% Yes 60% No; 40% stated that they are aware of the rules and security policies, and 60% said a lack of these regulations.
- In case of a disaster, do you know procedures for evacuating?
  50% Yes 50%; 50% No of respondents know the procedures for evacuation in case of a disaster because the signals have observed the building, the other 50% totally unknown and suggest that they are informed and prepare them performing a mock.
- Do you think if a disaster recovery plan is not executed the company will be paralyzed?
  100%; 100% of the 18 employees surveyed indicated that depend on the disaster and the affected area and that if only one party is to be paralyzed temporarily seek solutions.
- Do you know who the emergency team members are in a disaster?
  15% Yes 85% No; 15% said that if you have knowledge about the teams and the four employees who are responsible for its operation; 85% indicated that completely unknown about the equipment and its operation.
- Is a contingency plan the same as a disaster recovery plan?
  30% Yes 70% No; In this question 30% or 7 respondents say even the difference of these plans as they have been trained to handle these plans, whereas 70% say it is the same.
- Have you met the emergency team members for information retrieval of the recovery plan?
  100% No; officials know of the recovery plan, but who can imagine being in charge.
- Doe the staff know the company and the threats that may affect it?
  15% Yes 85% No; All respondents know the company: its representatives, departments, but when it comes to threats only 15% are aware of the different threats that may affect it, while 85% are unaware of the threats.

IT DISASTER RECOVERY PLAN (PROPOSAL)

Below details the elements that were part of the proposal and should not be ignored.

Statement of Intent

This document delineates our policies and procedures for technology disaster recovery, as well as our process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This document summarizes our recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of our people, our systems, and our data.

Our mission is to ensure information system uptime, data integrity and availability, and business continuity.

Policy Statement

Corporate management has approved the following policy statement [1]:

- The company shall develop a comprehensive IT disaster recovery plan.
- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
- The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be kept up to date to take into account changing circumstances.

All these elements are cyclic by nature which ensures continuous improvement of processes and therefore include a plan for more efficient disaster recovery as seen in Figure 1.

The principal objective of the disaster recovery program 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 information systems and business operations [2]. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan.
- The need to ensure that operational policies are adhered to within all planned activities.

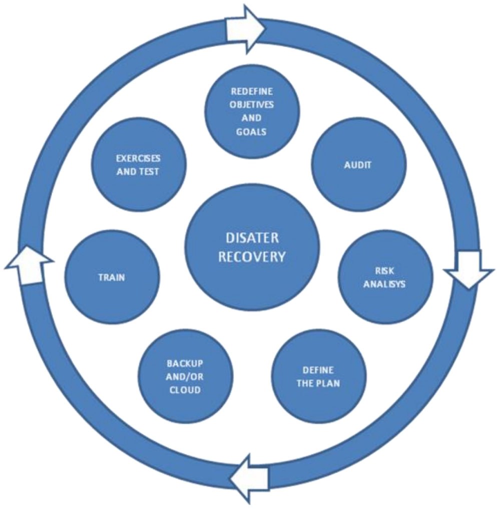

Figure 1
Disaster Recovery Cycle

Objectives

- The need to ensure that proposed contingency arrangements are cost-effective
- The need to consider implications towards other company sites
- Disaster recovery capabilities as applicable to key customers, vendors and others.

A detailed list of all key personnel Table 1 and the order of notification by phone Figure 2 should be established for the purpose of facilitating the activation of personnel in charge of recovery plan.

Table 1
Key Personnel Contact Info

Name	Title	Contact Option	Contact Number
Eugenio Perez	President	Work	787-000-0000
		Alternate	787-000-0000
		Mobile	787-000-0000
		Home	787-000-0000
		Email Address	eperez@company.biz
		Alternate Email	eperez@gmail.com
Fernando Garcia	Vice-President	Work	787-000-0000
		Alternate	787-000-0000
		Mobile	787-000-0000
		Home	787-000-0000
		Email Address	fgarcia@company.biz
		Alternate Email	fgarcia@yahoo.com
Maria Guerrero	Operation Manager	Work	787-000-0000
		Alternate	787-000-0000

Name	Title	Contact Option	Contact Number
		Mobile	787-000-0000
		Home	787-000-0000
		Email Address	mguerrero@company.biz
		Alternate Email	mguerrero@hotmail.com
Samuel Benitez	Network Manager	Work	787-000-0000
		Alternate	787-000-0000
		Mobile	787-000-0000
		Home	787-000-0000
		Email Address	sbenitez@company.biz
		Alternate Email	sbenitez@aol.com
Mateo Hernandez	Security and Infrastructure Manager	Work	787-000-0000
		Alternate	787-000-0000
		Mobile	787-000-0000
		Home	787-000-0000
		Email Address	mhernandez@company.biz
		Alternate Email	mhernandez@inbox.com
Miami Nelferd	International and External Services	Work	305-000-0000
		Alternate	305-000-0000
		Mobile	305-000-0000
		Home	305-000-0000
		Email Address	mnelferd@company.biz
		Alternate Email	mnelferd@att.com

Plan Overview

Take into account an overview on what elements should include the plan allows delimit its scope.

Plan Updating

It is necessary for the DRP updating process to be properly structured and controlled [3]. Whenever changes are made to the plan they are to be fully tested and appropriate amendments should be made to the training materials. This will involve the use of formalized change control procedures under the control of the Network Manager.

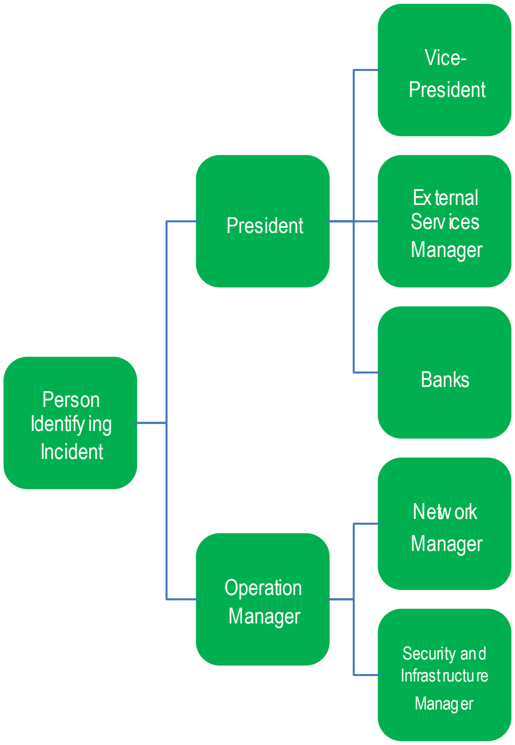
Vice-President
External Services Manager
Banks
President
Person Identifying Incident
Network Manager
Operation Manager
Security and Infrastructure Manager

Figure 2
Emergency Notification Calling Tree

Plan Documentation Storage

Copies of this Plan, CD, and hard copies will be stored in secure locations to be defined by the company. Each member of senior management will be issued a CD and hard copy of this plan to be filed at home. Each member of the Disaster Recovery Team and the Business Recovery Team will be issued a CD and hard copy of this plan. A master protected copy will be stored on specific resources established for this purpose [4].

Backup Strategy

Key business processes and the agreed backup strategy for each are listed below Table 2. The strategy chosen is for a fully mirrored recovery site at the company's offices in "Milla de Oro", Hato Rey. This strategy entails the maintenance of a fully mirrored duplicate site which will enable instantaneous switching between the live site (headquarters) and the backup site.

Table 2
Backup Strategy

KEY BUSINESS PROCESS	BACKUP STRATEGY
Network Manager	Fully mirrored recovery site
Tech Support - Hardware	Fully mirrored recovery site
Tech Support - Software	Fully mirrored recovery site
Facilities Management	Fully mirrored recovery site
Email	Cloud
Disaster Recovery	Fully mirrored recovery site
Finance	Fully mirrored recovery site
Contracts Admin	Fully mirrored recovery site
Product Sales	Fully mirrored recovery site
Maintenance Sales	Fully mirrored recovery site
Human Resources	Off-site data storage facility
Testing Fully Mirrored Recovery site -	Fully mirrored recovery site
Workshop Fully Mirrored Recovery site -	Fully mirrored recovery site
Call Center	Fully mirrored recovery site
Web Site	Cloud

Risk Management

There are many potential disruptive threats which can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included in this section, Table 3. Each potential environmental disaster or emergency situation has been examined. The focus here is on the level of business disruption which could arise from each type of disaster [5].

Potential disasters have been assessed as follows in the Table 3 about treats.

Emergency Response

Below sets out the elements that establish when they occur, how to deal with them and how it should operate the plan**.**

Plan Triggering Events

Key trigger issues at headquarters that would lead to activation of the DRP are:

- Total loss of all communications
- Total loss of power
- Loss of data
- Flooding of the premises
- Loss of the building

Table 3
Threats

Potential Disaster	Probability Rating	Impact Rating	Brief Description of Potential Consequences & Remedial Actions
Flood	3	4	All critical equipment is located on 2nd Floor
Fire	3	4	FM200 suppression system installed in main computer centers. Fire and smoke detectors on all floors.
Electrical storms	5		
Act of terrorism	5		
Act of sabotage	5		
Electrical power failure	3	4	Redundant UPS array together with auto standby generator that is tested weekly & remotely monitored 24/7. UPSs' also remotely monitored.
Loss of communications network services	4	4	Two diversely routed Ethernet port of 5 MB line into building. WAN redundancy, voice network resilience
Loss of Data	4	4	Cloud backup - daily basis

Probability: 1=Very High, 5=Very Low
Impact: 1=Total destruction, 5=Minor annoyance

Assembly Points & Emergency Exits

There are two emergency exits identified in the building. The first primary exit is located at the back of the building which is facing the backside of "Doña Fela" Parking Lot. The alternate emergency exit would be the one of the main entrance of the building.

Where the premises need to be evacuated, the DRP invocation plan identifies two evacuation assembly points:

- Primary – “Doña Fela” Parking lot of company across the street
- Alternate – The main entrance door of the building.

Activation of Emergency Response Team

When an incident occurs the Emergency Response Team (ERT) must be activated. The ERT will then decide the extent to which the DRP must be invoked. All employees must be issued a Quick Reference card containing ERT contact details to be used in the event of a disaster. Responsibilities of the ERT are to:

- Respond immediately to a potential disaster and call emergency services;
- Assess the extent of the disaster and its impact on the business, data center, etc.;
- Decide which elements of the DR Plan should be activated;
- Establish and manage disaster recovery team to maintain vital services and return to normal operation;
- Ensure employees are notified and allocate responsibilities and activities as required.

Disaster Recovery Team

The team will be contacted and assembled by the ERT. The team's responsibilities include:

- Establish facilities for an emergency level of service within 2.0 business hours;
- Restore key services within 4.0 business hours of the incident;
- Recover to business as usual within 8.0 to 24.0 hours after the incident;
- Coordinate activities with disaster recovery team, first responders, etc.
- Report to the emergency response team.

Emergency Alert, Escalation and DRP Activation

This policy and procedure has been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications can be quickly established while activating disaster recovery.

The DR plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology and business recovery. Suppliers of critical goods and services will continue to support recovery of business operations as the company returns to normal operating mode.

Emergency Alert

The person discovering the incident calls a member of the Emergency Response Team in the order listed.

The Emergency Response Team is composed of following people:

- President
- Operation Manager

If not available try:

- Vice-president

The Emergency Response Team (ERT) is responsible for activating the DRP for disasters identified in this plan, as well as in the event of any other occurrence that affects the company’s capability to perform normally.

One of the tasks during the early stages of the emergency is to notify the Disaster Recovery Team (DRT) that an emergency has occurred. The notification will request DRT members to assemble at the site of the problem and will involve sufficient information to have this request effectively communicated. The Business Recovery Team (BRT) will consist of senior representatives from the main business departments. The BRT Leader will be a senior member of the company's management team, and will be responsible for taking overall charge of the process and ensuring that the company returns to normal working operations as early as possible.

DR Procedures for Management

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.

Contact with Employees

Managers will serve as the focal points for their departments, while designated employees will call other employees to discuss the crisis/disaster and the company's immediate plans. Employees who cannot reach staff on their call list are advised to call the staff member's emergency contact to relay information on the disaster.

Backup Staff

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.

Recorded Messages / Updates

For the latest information on the disaster and the organization's response, staff members can call a toll-free hotline listed in the DRP wallet card. Included in messages will be data on the nature of the disaster, assembly sites, and updates on work resumption.

Alternate Recovery Facilities / Hot Site

If necessary, the hot site at "X" Company will be activated and notification will be given via recorded messages or through communications with managers. Hot site staffing will consist of members of the disaster recovery team only for the first 24 hours, with other staff members joining at the hot site as necessary.

Personnel and Family Notification

If the incident has resulted in a situation which would cause concern to an employee's immediate family such as hospitalization of injured persons, it will be necessary to notify their immediate family members quickly.

Media

Working with the media, as well as establish restrictions channels and allows the flow of information to the public clearly.

Media Contact

Assigned staff will coordinate with the media, working according to guidelines that have been previously approved and issued for dealing with post-disaster communications.

Media Strategies

Define how you should handle the media is extremely beneficial for the image of the organization, should take into account the following elements:

- Avoiding adverse publicity
- Take advantage of opportunities for useful publicity
- Have answers to the following basic questions:
  - What happened?
  - How did it happen?
  - What are you going to do about it?

Media Team

The peoples who will make up the team to work with the media should be composed of Vice-president and Operation Manager.

Rules for Dealing with Media

Only the media team is permitted direct contact with the media; anyone else contacted should refer callers or in-person media representatives to the media team.

Insurance

As part of the company's disaster recovery and business continuity strategies a number of insurance policies have been put in place. These include errors and omissions, directors & officers liability, general liability, and business interruption insurance.

If insurance-related assistance is required following an emergency out of normal business hours, must indicate the name of the contact person.

A list of the different information policies that owns the company has to drawn up and should include the following elements:

- Policy Name
- Coverage Type
- Coverage Period
- Amount Of Coverage
- Person Responsible For Coverage
- Next Renewal Date

Financial and Legal Issues

Events are related to legal and financial issues have updated information on the subject and enlist the help of consultants helps to have a more precise idea of the event and give us a starting point when it comes to recover.

Financial Assessment

The emergency response team shall prepare an initial assessment of the impact of the incident on the financial affairs of the company [6]. The assessment should include:

- Loss of financial documents
- Loss of revenue
- Theft of check books, credit cards, etc.
- Loss of cash

Financial Requirements

The immediate financial needs of the company must be addressed. These can include:

- Cash flow position.
- Temporary borrowing capability.
- Upcoming payments for taxes, payroll taxes, Social Security, etc.
- Availability of company credit cards to pay for supplies and services required post-disaster.

Legal Actions

The company legal consultant and ERT will jointly review the aftermath of the incident and decide whether there may be legal actions resulting from the event; in particular, the possibility of claims by or against the company for regulatory violations, etc.

DRP Exercising

Disaster recovery plan exercises are an essential part of the plan development process. In a DRP exercise no one passes or fails; everyone who participates learns from exercises – what needs to be improved, and how the improvements can be implemented. Plan exercising ensures that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities.

Successful DR plans launch into action smoothly and effectively when they are needed. This will only happen if everyone with a role to play in the plan has rehearsed the role one or more times. The plan should also be validated by simulating the circumstances within which it has to work and seeing what happens.

Revision History

Must contain every time you make a revision to disaster recovery plan document:

- Revision
- Date
- Name
- Description

CONCLUSIONS

Taking into account the information collected and analyzing it we could get the following:

- There is no plan [7].
- It has operations and alternative equipment places.
- No guides and disaster procedures.
- The staff has no knowledge about how to act in case of disaster.
- The staff does not see a correlation between the type of service that is provided and how to continue the same in case of disasters.
- Potential causes of interruption of the company activities would flood, fire, loss communication and servers down
- The availability of resources would be affected by power failures, communications failure,

equipment failure, internal power failure, air conditioning, incidents of information security, cyber-attacks, unauthorized access data losses, failures events triggered systems sabotage, vandalism, theft, arson.

RECOMMENDATIONS

Considering the findings in the reality of the company we recommend that:

- Audits are recommended because the earlier an audit takes place, the greater, and the benefits for the company.
- You need to keep the entire organization constantly updated with the processes described above in the proposal so that they are applied with a semiannual basis. This way everyone involved in the plan are properly prepared and trained in this process of constant renewal to the plan.
- You must be very careful when analyzing threats and vulnerabilities of these systems, in order to establish a real and objective way to minimize the possible losses and damages based on the probability to occur.
- Specify guidelines and procedures to follow in case of a disaster.
- Educate and train staff in the event of a disaster.
- Improve the electrical infrastructure and the backup's facilities.

REFERENCES

[1] Paul, D, "In Its wake, Hurricane Sandy left Disaster Recovery Lessons", *Disaster Recovery Journal,* Vol. 26 No.2, Spring 2013, 20-22.

[2] Gaudreau, B, "A Dynamic Plan to Minimize Disaster Downtime", *Disaster Recovery Journal,* Vol. 26 No.2, Spring 2013, 28-30.

[3] IBM (2012, Jun). White Paper: Business Continuity and Resiliency Services. Retrieved January 3, 2013, from http://www-935.ibm.com/services/us/en/it-services/business-continuity-and-resiliency-services.html

[4] Schiesser, R, "Chapter 17 Business Continuity", *IT System management,* Pearson Education, 2010, 241-258.

[5] FEMA (2012 Oct 25). IT Disaster Recovery Plan, Retrieved January 10, 2013, from http://www.ready.gov/business/implementation/IT.

[6] SBA (2012). Disaster Recovery Plan, Retrieved January 10, 2013, from http://www.sba.gov/content/disaster-preparedness-and-recovery-plan.

[7] Casey, K, "57% Of SMBs Have No Disaster Recovery Plan", *Information Week*, January , http://www.informationweek.com/smb/security/57-of-smbs-have-no-disaster-recovery-pla/229000461, 2011