
Disaster Recovery Plan Proposal

Children's Campaign, Inc.

Daniel Freeman, Yaniv Levy, Clint Morrow, Michael Murray
Final Report • January 29, 2009



Table of Contents



Project Summary	3
Executive Summary	3
Handoff Plan	4
Lessons Learned	6
Final Project Plan	7
Project Charter	7
Goal Breakdown Schedule	8
Scope of Work	9
Risk Assessment	10
Constraints and Assumptions	13
Project Documents	14
Project Budget	14
Work Breakdown Schedule	15
Sponsor Acceptance and Evaluation Form	25
Deliverables	26

Project Summary

EXECUTIVE SUMMARY

Overview

There are many common risks involved in all business environments that can lead to adverse effects and hinder company growth. These risks can come from external sources such as natural disasters including hurricanes, tornadoes, floods, and such as well as internal risks including hardware failure, human error, or even sabotage. It is essential for a company to create and follow business policies to secure the integrity of information as well as various company assets crucial to company functionality. A Disaster Recovery Plan (DRP) is an integral part of a business policy and ensures the integrity and functionality in case of a disaster.

Problem

Currently, there is no Disaster Recovery Plan implemented at Children's Campaign. Having already suffered a disruption in service due to hardware related failure of integral system componentry and loss of sensitive data, methods must be taken to ensure this type of failure does not occur again.

Solution

The technology team has taken the initiative in creating and implementing a DRP to minimize necessary risks, increase the dependability of the computer systems being used, and create specific strategies in case of disruption or disaster. Measures have been taken to cover all points of possible risk. Precautions are taken at both the hardware and software levels to maintain system functionality and protect the IT infrastructure. As part of the DRP, Children's Campaign personnel will be educated on how to properly use their computer systems and become aware of possible security threats. Scenarios related to possible risks have been analyzed and strategies have been created as a precaution. Proper implementation of the DRP will create a solid, secure foundation and maximize productivity in the organization.

HANDOFF PLAN

In order for the success of the project to continue, a project handoff plan has been established, which is comprised of Familiarizing Documents, Document Storage Locations, and a schedule outlining the various phases the project will undergo.

Familiarizing Documents

This document in its entirety will serve as the basis for future employees to acquaint themselves with the Disaster Recovery Plan. This final project plan serves as a comprehensive collection of documents to introduce the problem and familiarize them with the actions that have already taken place as well as the ones planned. The Wiki, mentioned below, will serve as the central location for coordination and communication for all activities currently being addressed.

Document Storage Locations

This document, along with the finalized versions of the project deliverables will be stored in both hard-copy format as well as to be available on Children's Campaign's Public Library file server. In addition, a Wiki section will be created and serve as the primary repository for future disaster recovery project updates.

The following are the logical file locations for the various documents:

- X:\Technology\Disaster Recovery Policy (**CC Public Library**)

** Accessible to end-users, sponsor, and project members*

- <http://systemone/mediawiki/> (**Technology Wiki on Intranet**)

** Accessible to sponsor and project members*

Project Phases

Phase 1 - Disaster Recovery Plan Formation and Establishment

Phase 1 has been in progress and will be formally completed with the conclusion of this document. It establishes the basis for all future planning and provides a common framework for subsequent project members to work with.

Phase 2 - Policy Writing

Phase 2 is expected to start in January of 2009. This phase will expand on phase 1 by writing all of the proposed policies established in the work breakdown schedule. Once these policies are in place, the project can move forward to the implementation phase.

Phase 3 - Equipment Purchasing and Implementation

Phase 3 is comprised of all equipment purchasing and policy implementation that has not already been completed. This phase marks the beginning of the project's measurable impact on the organization. As each equipment and policy is implemented, the organization will start to see the benefits proposed by the disaster recovery policy.

Phase 4 - Testing

Upon completion of phase 3, phase 4 will be testing of various recovery techniques outlined in the work breakdown schedule. This phase is intended to work out various inconsistencies, inadequacies, and other factors that were unknown or unable to be accounted for. In other words, this phase will focus on refining the techniques and policies established in phase 2 and 3.

Phase 5 - Maintenance and Upkeep

Because Children's Campaign is an organization that continually grows and changes, the disaster recovery policy must be continually updated and revised to meet such changes. This phase is intended to be revisited biannually in May and November. All documents, including the Wiki, are to be revisited and all of the organization's factors should be considered and then revised.

LESSONS LEARNED

During the course of this project we learned many useful things about about project management, our project, and even ourselves.

Time Estimations

We started the Disaster Recovery Plan under the impression that we would fully complete the plan in the span of four months. We had no idea how in-depth this process would be and ended up scaling the project back. At the end of this project, we had a pretty good impression of how long it takes to get certain tasks done and will be better for future projects.

Project Management

At the start of this project, our group members all brought varying levels of project management skills. We had little idea how to manage a project or how to plan a plan. We had a mock project beforehand but that was not enough preparation for the real project. Over the span of this project and semester, we learned a lot about project management but we feel more experience its always better.

High Expectations

Another lesson we learned is that expecting too much out of everyone will lead to disappointment. We are all different and each team member's capacity to add value to this project is different, but that does not mean it is less. Some of us thought that others should be doing more work, or helping out more, and that can't always happen. We learned to work around everyones schedule and assign tasks to those who do them best.

Use of Software

During this project we used Microsoft Project for the Work and Goal Breakdown Schedules. Our Work Breakdown Schedule (WBS) was extremely long and complicated. Not much information can be captured in the program apart from schedules. We realized that supporting documents were needed to explain the task items in further detail. In the future, we will analyze the usefulness of certain pieces of software for their strengths and weakness before depending too heavily on them.

These were only a few of the many other lessons we learned from this project. We cannot hope to capture all the useful concepts we learned in this document.

Final Project Plan

PROJECT CHARTER

Children's Campaign, a political advocacy organization who focuses on serving children's issues, intends to create a comprehensive Disaster Recovery Plan to help recover from potential disasters in the event the organization were to experience such.

As the organization currently stands, there is no Disaster Recovery Plan. Merely, only limited remote backup procedures are in place to protect intellectual property, namely the public file server documents and e-mail. While this is a large step forward, it does not comprehensively secure the organization's technology infrastructure in a recognized fashion.

Two years ago, the organization suffered from complete server failure in which all data was unable to be recovered. This plan serves to keep such instances from happening as well as preventing disasters on an even larger scale from completely destroying the organization's intellectual property. As a result, this plan will substantially reduce the organization's downtime in such an event.

Due to the nature of the organization, this project is intended to be an ongoing effort beginning in Fall 2008 and continuing until the policy is completely implemented. Children's Campaign will be working with FSU College of Information interns. Currently, it is being implemented by the current Technology Interns Daniel Freeman, Yaniv Levy, Clint Morrow and Michael Murray. The Technology Consultant, Melissa Raulston and Project Sponsor/Executive Director, Linda Alexionok, oversee the policy.

GOAL BREAKDOWN SCHEDULE

- 1) Secure the organization's assets
 - a) Tangible assets
 - b) Intangible assets, including intellectual property
- 2) Establish data redundancy measures
 - a) Backup measures for hardware failure
 - b) Backup measures for user error
- 3) Improve operational efficiency
 - a) Operational policies to improve user performance
 - b) Physical policies for improved security
 - c) Management policies for improved management

SCOPE OF WORK

The Disaster Recovery Plan to be implemented is intended to cover all aspects Children's Campaign. More specifically, the Disaster Recovery Plan will consider aspects extending beyond information technology. This includes areas of the organization but not limited to: human resource information, communications, non-technological assets including paper documents, media of any type, tangible assets such as office furniture and equipment, intellectual property, company policies and procedures, etc.

Children's Campaign, Inc.'s scope extends beyond the walls of the Tallahassee office. Also to be considered is all external relations in the recovery process. For example, off-site employees, board members, sponsors, and clients will still need to function in the event of a disaster. Plans need to be in place to allow the mentioned to continue functioning, perhaps reduced, in order to continue the organization's mission and goal while recovery efforts are underway.

Ensuring that all aspects of the organization is a daunting and comprehensive task, so the items mentioned are only a preliminary plan. This document is intended to evolve over the course of the project in order to successfully consider 100% of the organization.

RISK ASSESSMENT

Risk	Probability	Impact	Product	Mitigation	Task Changes
Data Loss	7	10	Worker ability to perform his or her tasks	Ensure complete data backup	Account for more data backup planning
Failure to recognize aspects impacted	5	7	Loss of company assets	Verify project plan scope and thoroughness	Invest more time in analyzing project needs
Unapproved task items affecting project outcome	6	8	Efficient recovery from disaster / Loss of company assets	Verify with sponsor the necessity for items	Create alternative solutions to account for unapproved task items
Loss of productivity	9	10	Worker ability to perform his or her tasks	Reduce downtime and recovery through detailed and thorough planning	Rehearse Disaster Recovery Plan

Risk	Probability	Impact	Product	Mitigation	Task Changes
Loss of company revenue	9	10	Company mission	Reduce downtime and recovery through detailed and thorough planning	Rehearse disaster recovery plan
Server Failure	5	10	Companies entire technological infrastructure	Run server maintenance to insure stability	Account for changes in tasks to allow for server maintenance
Break in	7	10	Potential loss of important resources critical for operation	Implement security system and verify doors are locked after business hours	Develop physical security prevention measures
Flood	1	10	Potential loss of important resources critical for operation	Move important resources off of the floors	Account for flood in disaster recovery plan

Risk	Probability	Impact	Product	Mitigation	Task Changes
Fire	5	10	Potential loss of important resources including the building	Implement fire-safe boxes, verify kitchen equipment if off after business hours	Account for fire in disaster recovery plan
Incorrect packages delivered	4	6	Loss of time having to return and reorder items	Verify package is correct before the deliverer leaves	None
Loss of keys	6	8	Unable to unlock various doors, opens risk of break in	Keep keys off main key-chain, verify they are still in possession	Having to change locks, may affect work schedule

CONSTRAINTS AND ASSUMPTIONS

Assumptions

- Our project sponsor is willing to approve our proposals and recommendations.
- No disasters will occur during the planning of the Disaster Recovery Plan.
- The organization's structure and size will not change drastically over the coming months.
- Market issues will not greatly impact spending on disaster recovery.

Constraints

- Systems infrastructure is limited in capability: bandwidth for off-site backup can only be done incrementally.
- Project budget is limited: non-profit organizations do not have a large expendable cash flow to work with.
- Implemented equipment and processes cannot greatly impact normal business operations.

Project Documents

PROJECT BUDGET

Item	Purpose	Price
DVD Backups	Protect software and generated files	\$150
Fire Safe Box	Protect tangible assets	\$1,300
Hard Drives	Duplicate systems to allow speedy recovery	\$800
Security Fund	To quickly purchase equipment or resources in time of crisis	\$5,000
Maintenance	Keep equipment and backups running smoothly	\$300
Unforeseen Costs	To account for budget for unforeseen changes in tasks, or problems during implementation of the Disaster Recovery Plan	\$2,500
Total		\$10,000

WORK BREAKDOWN SCHEDULE

- 1 Children's Campaign Disaster Recovery Plan
 - 1.1 Pre Planning Activities
 - 1.1.1 Establish communication plan
 - 1.1.1.1 Establish contact methods
 - 1.1.1.2 Establish reporting methods
 - 1.1.1.3 Establish reporting intervals
 - 1.1.2 Develop schedules
 - 1.1.2.1 Establish group meeting times
 - 1.1.2.2 Establish meeting intervals
 - 1.1.3 Identify factors that could have impact of success of project
 - 1.1.3.1 Consider time
 - 1.1.3.1.1 Compare schedules of tech team
 - 1.1.3.1.2 Estimate time spans for each phase of project
 - 1.1.3.1.3 Extend time as necessary
 - 1.1.3.1.4 Consider cost
 - 1.1.3.1.4.1 Labor
 - 1.1.3.1.4.2 Budget Limit
 - 1.1.3.1.4.3 Downtime
 - 1.1.3.1.4.4 Unexpected Expenditures
 - 1.1.3.2 Unexpected logistics
 - 1.1.3.2.1 Availability of parts
 - 1.1.3.2.2 Delivery Time
 - 1.1.3.2.3 Compatibility

- I.1.3.2.4 Faulty Parts
- I.1.4 Meet with sponsor
 - I.1.4.1 Analyze business needs for Disaster Recovery Plan
 - I.1.4.2 State reason(s) for Disaster Recovery Plan
 - I.1.4.3 Establish which sectors of organization are to be included
 - I.1.4.4 Establish time frame requirements for recovery process
 - I.1.4.5 Establish which facets are mission critical, secondary, and tertiary
 - I.1.4.5.1 Discuss important assets to be secured
 - I.1.4.6 Differentiate tangible/intangible information to be secured
 - I.1.4.6.1 Discuss where tangible resources is to be stored
 - I.1.4.6.2 Discuss where intangible data is to be stored
- I.1.5 Analyze budget
 - I.1.5.1 Establish income sources
 - I.1.5.2 Approximate total budget for project
 - I.1.5.3 Approve budget
- I.1.6 Refine project scope
 - I.1.6.1 Establish cost constraints
 - I.1.6.2 Establish project feasibility and viability
 - I.1.6.3 Estimate timeframe of all project phases
- I.2 Vulnerability Assessment and General Definition Requirements
 - I.2.1 Create Policies
 - I.2.1.1 Management/Informational Policies
 - I.2.1.1.1 Workstation upgrade schedule policy
 - I.2.1.1.2 Equipment auditing policy

1.2.1.1.3	Insurance policy
1.2.1.1.4	Develop information classification matrix policy
1.2.1.1.4.1	Private information
1.2.1.1.4.2	Public information
1.2.1.1.4.3	Internal information
1.2.1.1.4.4	Confidential information
1.2.1.2	Operational Policies
1.2.1.2.1	Data backup policy
1.2.1.2.1.1	Verify space requirements for Exavault
1.2.1.2.1.2	Verify bandwidth requirements for Exavault
1.2.1.2.1.3	Verify Exavault remote backup schedule
1.2.1.2.1.4	Verify Exavault remote backup items
1.2.1.2.1.5	Evaluate bandwidth requirements
1.2.1.2.1.6	Evaluate backup space requirements
1.2.1.2.1.7	Evaluate need for additional backup methods
1.2.1.2.2	Server/Workstation Monitoring Policy
1.2.1.2.2.1	Evaluate need for an Intrusion Detection System
1.2.1.2.2.2	Consider database security
1.2.1.2.2.3	Consider data and voice communications security
1.2.1.2.2.4	Consider systems and access control software security
1.2.1.2.3	Email Usage Policy
1.2.1.2.4	Internet Usage Policy

1.2.1.2.5	File Storage/Retrieval Usage Policy
1.2.1.2.6	Systems Maintenance Policy
1.2.1.2.6.1	Develop automated virus/malware scan schedule
1.2.1.2.6.2	Develop email archival policy
1.2.1.2.6.3	Develop monthly hardware diagnostic policy
1.2.1.2.7	Conduct awareness sessions
1.2.1.3	Physical Policies
1.2.1.3.1	Server Room Policy
1.2.1.3.1.1	Establish which items are in server room
1.2.1.3.1.2	Establish need for server room equipment
1.2.1.3.1.3	Establish temperature control measures
1.2.1.3.2	Building Access Policy
1.2.1.3.2.1	Establish who has access to building after-hours
1.2.1.3.2.2	Re-evaluate on a need-basis
1.2.1.3.2.3	Consider employees privy to building and server room keys
1.2.1.3.3	Fire Safe Box Policy and Usage
1.2.1.3.3.1	Evaluate current fire safe boxes
1.2.1.3.3.2	Evaluate need for upgraded equipment
1.2.1.3.3.3	Write plan proposal
1.2.1.3.3.4	Get approval
1.2.1.3.3.5	Document the decision
1.2.1.3.3.6	Implement if approved
1.2.1.3.4	Workstation Security Policy

- I.2.I.3.4.1 hardware Create inventory and documentation for all
- I.2.I.3.4.2 Create workstation usage policy
- I.3 Business Impact Assessment
 - I.3.1 Prepare draft report
 - I.3.1.1 Consider all critical systems
 - I.3.1.2 Consider all processes and functions
 - I.3.1.3 Consider economic impact of incidents and disasters
 - I.3.1.4 Assess "pain threshold" - length of time business units can survive without access to systems, services, and facilities
 - I.3.2 Prepare final report
 - I.3.3 Present report to project team and sponsor
- I.4 Detailed Definition and Requirements
 - I.4.1 Record mission critical credentials and resources
 - I.4.1.1 Record internet service provider vendor
 - I.4.1.2 Record phone system vendor
 - I.4.1.3 Record data backup provider
 - I.4.1.4 Record fax provider
 - I.4.1.5 Record electricity vendor
 - I.4.1.6 Record administrator login credentials
 - I.4.1.7 Record paper copy of knowledgebase and wiki
 - I.4.1.8 Record employee contact information
 - I.4.2 Record secondary resources
 - I.4.2.1 Software discs
 - I.4.2.2 Electronic files and intellectual property

- I.4.2.3 Files in conference room
- I.4.2.4 Pattie's file cabinets
- I.4.2.5 Linda's file cabinet
- I.4.2.6 Raquel's file cabinet
- I.4.2.7 Jennifer's file cabinet
- I.4.2.8 Windows server
- I.4.2.9 Linux server
- I.4.2.10 Computers
- I.4.2.11 Copy/printer/scanner machine
- I.4.2.12 Phone system
- I.4.2.13 Computer accessories
- I.4.2.14 APC and surge protectors
- I.4.2.15 External DVD burner
- I.4.2.16 Furniture
- I.4.2.17 Office supplies
- I.4.3 Record tertiary/non-essential resources
 - I.4.3.1 Decorations
 - I.4.3.2 Kitchen Appliances
 - I.4.3.3 Kitchen Utensils
- I.4.4 Asses backup office locations
 - I.4.4.1 Asses cost
 - I.4.4.2 Asses location
 - I.4.4.3 Asses size
 - I.4.4.4 Asses availability

1.4.4.5	Asses timeframe	
1.4.5	Assessed Requirements	
1.5	Plan Development and Precautionary Measures Implementation	
1.5.1	Implement developed policies	
1.5.1.1	Management policies	
1.5.1.1.1	Implement upgrade schedule policy	
1.5.1.1.1.1	Begin initial workstation upgrade interval (first time only)	
1.5.1.1.1.1.1	interval	Prepare proposal for initial upgrade
1.5.1.1.1.1.2	interval	Submit proposal for initial upgrade
1.5.1.1.1.1.3		Document decision
1.5.1.1.1.1.4		Implement workstation upgrades
1.5.1.1.1.2	Continue workstation upgrade interval (successive times)	
1.5.1.1.1.2.1	grade interval	Prepare proposal for subsequent up-
1.5.1.1.1.2.2	grade interval	Submit proposal for subsequent up-
1.5.1.1.1.2.3		Document decision
1.5.1.1.1.2.4		Implement workstation upgrades
1.5.1.1.2	Implement equipment and auditing policy	
1.5.1.1.3	Implement information classification matrix	
1.5.1.1.3.1		Tag existing documents using developed schema
1.5.1.1.3.2	creation	Implement tagging policy for new document

1.5.1.1.3.2.1		Train employees on tagging documents
1.5.1.2	Operational policies	
1.5.1.2.1	Implement backup policy	
1.5.1.2.1.1	Purchase backup equipment	
1.5.1.2.1.1.1	Purchase backup drives	
1.5.1.2.1.1.2	Purchase backup media	
1.5.1.2.1.1.3	Back up data	
1.5.1.2.1.1.3.1	Assign a particular Tech Team member to check, validate, and maintain backups	
1.5.1.2.1.1.3.2	Create redundant server states	
1.5.1.2.1.1.3.3	Organize and consolidate software collection	
1.5.1.2.1.1.3.4	Create redundant copies of backups for storage offsite	
1.5.1.2.2	Implement server/workstation monitoring policy	
1.5.1.2.2.1	Prepare proposal for purchase of software and monitoring equipment	
1.5.1.2.2.2	Submit proposal	
1.5.1.2.2.3	Document decision	
1.5.1.2.2.4	Implement software/equipment	
1.5.1.2.3	Implement email usage policy	
1.5.1.2.4	Implement internet usage policy	
1.5.1.2.5	Implement file storage/retrieval usage policy	
1.5.1.2.6	Implement systems/maintenance policy	

- 1.5.1.2.6.1 Implement automated virus scan policy
- 1.5.1.2.6.2 Implement email archival policy
- 1.5.1.2.6.3 Implement monthly hardware diagnostics policy
- 1.5.1.3 Physical policies
 - 1.5.1.3.1 Implement server room policy
 - 1.5.1.3.2 Implement building access policy
 - 1.5.1.3.3 Implement Fire Safe Box policy
 - 1.5.1.3.3.1 Purchase Fire Safe Box
 - 1.5.1.3.3.2 Store assets determined previously in Fire Safe Box
 - 1.5.1.3.4 UPS Policy
 - 1.5.1.3.4.1 Purchase UPS equipment
 - 1.5.1.3.4.2 Install UPS equipment
 - 1.5.1.3.5 Implement workstation security policy
 - 1.5.1.3.6 Offsite policy
 - 1.5.1.3.6.1 Store secondary copies of software offsite
- 1.5.2 Precautionary Measures Completed
- 1.6 Testing Program
 - 1.6.1 Execute test disaster scenario
 - 1.6.1.1 Assess disaster
 - 1.6.1.2 Contact executive director
 - 1.6.1.2.1 Discuss damages
 - 1.6.1.2.2 Discuss solutions
 - 1.6.1.3 Implement solutions
 - 1.6.1.3.1 Refer to policies

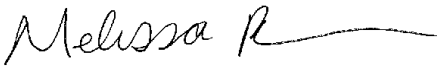
- 1.7 Maintenance and Control Measures
 - 1.7.1 Ensure DRP is updated on yearly basis
 - 1.7.2 Check budget on weekly intervals
- 1.8 Plan Closure
 - 1.8.1 Finalize Risk Assessments
 - 1.8.2 Finalize Budget
 - 1.8.3 Submit disaster recovery report
 - 1.8.4 Present to management

SPONSOR ACCEPTANCE AND EVALUATION FORM

Project Name: Disaster Recovery Plan

Project Manager: Clint Morrow

I (We), the undersigned, acknowledge and accept delivery of the work completed for this project on behalf of our organization. My (Our) signature(s) attest(s) to my (our) agreement that Phase 1 of this project has been completed.

Name	Title	Signature	Date
Melissa Raulston	Project Sponsor		Nov 25, 2008

1. Was this project completed to your satisfaction? Yes No

2. Please provide the main reasons for your satisfaction or dissatisfaction with this project.

The project was thoroughly and completely scoped and scrutinized with superb attention to detail. All aspects of operations were analyzed and input was gathered from all affected stakeholders. Additionally, the team sought outside input on their plan by consulting with other senior systems administrators with DRP responsibilities including Casey McLaughlin.

3. Please provide suggestions on how our organization could improve its project delivery capability in the future.

I have no suggestions for improvement. The plan was executed as well as humanly possible while juggling the competing responsibilities of other classes and a 6-hour DIS on the part of two of the team members. In spite the pressures of class and work, this team produced a stellar result that will go into production during the Spring semester. There is no higher compliment to the work of this team than to get the sign-off of senior managers at Children's Campaign to proceed with the implementation.

DELIVERABLES

- Project Charter
- Project Plan
- Work Breakdown Schedule
- Risk Assessment
- Project Budget
- Handoff Plan
- Sponsor Evaluation