ARE NONPROFIT ORGANIZATIONS READY FOR THE NEXT BIG (OR LITTLE) DISASTER? 7-STEPS TO STRAIGHT FORWARD CONTINUITY PLANNING AND DISASTER RECOVERY

Sandra Blanke
University of Dallas Graduate School of Management
7460 Warren Parkway, Suite 100
Frisco, TX 75034
(972) 265-5724
(972) 265-5750 Fax
sandrablanke@cablerocket.com

Elizabeth McGrady
University of Dallas Graduate School of Management
1845 East Northgate Drive
Irving, TX 75062-4736
(972) 721-5097
(972) 721-5265 Fax
emcgrady@gsm.udallas.edu

ABSTRACT

Nonprofit organizations fill critical roles in disaster response, however, focus on client needs and scarce resources divert attention to effective continuity and disaster recovery planning. This article describes a straightforward 7-step approach that will help nonprofit organizations expediently build a proven continuity and disaster recovery plan to increase organizational readiness. The steps include: assessing current readiness level, risk analysis, impact analysis, emergency response planning, organizational resumption planning, plan testing and auditing, and maintenance.

INTRODUCTION

The priority focus of nonprofit (NP) managers is taking care of client needs and securing resources to fund services. Since client needs such as health services, food services, housing and other essential services may be critical to livelihood managers may resist diverting attention to longer term organizational needs such as continuity planning and disaster recovery. However, these management functions can help ensure sustainability and mitigate the interruption of services (Meyer-Emerick & Momen, 2003). Disasters take many forms and may be big such as fire and major weather events or small such as loss of power. The need for response may involve a disaster at the organization's location, or be in response to an event in a distant locale, such as the Texas cities response to the Katrina evacuation. Adequate continuity and disaster response planning can assure that NP organizations are able to serve their clients even during adverse situations.

In a recent study (Blanke & McGrady, 2007) 96% of NP managers surveyed acknowledged the need for continuity planning and disaster recovery training. Continuity planning was deemed to be a critical success factor in supporting clients in times of disaster. The top continuity planning need was for overall training. The open-ended responses for training and preparation needs are listed in Table 1 with response frequency.

Training Preparation Needs	Per Cent
Overall planning training	50.0
Communication during disaster	14.6
Development of plans	10.4
Ability to coordinate and link with other organizations	10.4
Ability to find resources	6.3
Internal prioritization and coordination	6.3
Evacuation/relocation	2.0

Table 1: List of training preparation needs

The University of Dallas Information Assurance program and Nonprofit Leadership Institute used the survey results to develop a NP Continuity Planning (CP) training tool. The tool was tested with Dallas area NP agencies (Blanke & McGrady, 2007). The seven step CP training tool includes the following items in sequential order:

- Step 1 - Assess the readiness level of the NP agency
- Step 2 - Determine likely risk
- Step 3 - Conduct an impact analysis (IA)
- Step 4 - Develop an emergency response
- Step 5 - Create an organizational resumption plan
- Step 6 - Test and audit the plan
- Step 7 - Perform plan maintenance.

Continuity planning is an ongoing process and requires reassessment at least annually or when significant changes occur in the organization. CP focuses on "providing methods and procedures for dealing with longer-term outages and disasters", (Harris, 2005). It may be described as the time when it is realized that the sky has fallen – how do we stay in business, take care of our clients, keep going and put the sky back where it belongs (Harris). CP includes:

- Taking a longer look at the problem
- Getting the right people to the right places
- Offering service in a different mode until normal conditions are back in place
- Responding to clients, volunteers, board members, vendors and others through different channels until normality returns.

The diagram below is provided to depict the actual steps in a circular and continuous flow.

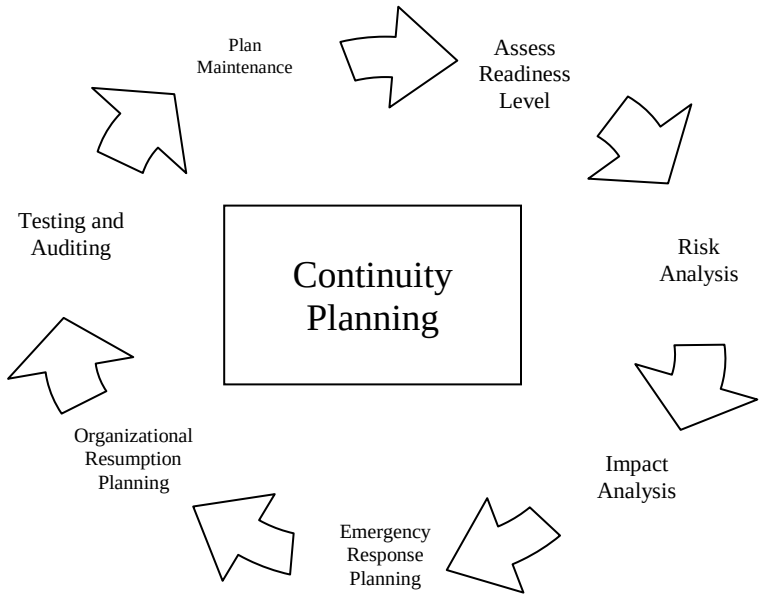

Diagram 1: 7 Steps to Straight Forward Continuity Planning

Assess Readiness Level – Step 1

In a 2007 study (Blanke & McGrady) 60% of respondents reported they had a continuity and disaster recovery plan in place, while 40% did not. Though organizations had a plan, only 13% had reviewed, updated, and tested the plan in the last year. There is a critical difference in having a plan and thoroughly implementing the planning process.

The recommended first step of the plan is for organizations to assess their preparedness (readiness) for a disaster. This can be accomplished by measuring their Readiness Index score on the 14 item list below. The score is measured by an affirmative response to completion of each of the following items.

1. Having a disaster recovery plan in place
2. Identification of threats
3. Identification of probabilities of threats
4. Identification of vulnerabilities
5. Identification of potential impact of vulnerabilities
6. Annual review of plan
7. Annual update of plan
8. Annual testing of plan
9. Key contact list
10. Electronic storage of plan
11. Location of plan known by multiple staff
12. Location of alternate location of conducting services
13. Repair and service contract
14. Communication of plan with reciprocal agencies

The mean score for the Readiness Index in the 2007 (Blanke & McGrady) study was 6.2 out of the possible score of 14.0 indicating that though organizations have initiated the continuity and disaster planning process there is still work to be done for most organizations. Organizations can use the Readiness Index as a means of charting and communicating progress. Communities can use the Readiness Index to track the overall preparedness level and to identify areas of vulnerability and additional training needed.

Risk Analysis – Step 2

The next step is to complete a risk analysis. Risk is defined as the possibility of a person or entity suffering harm or loss (Wells, Walker & Walker, 2007). Risk analysis is the process of analyzing threats and vulnerabilities (Whitman & Mattord, 2007). There are four strategies for managing or mitigating risk based on the risk priority. The strategies are; avoidance, correction, transference, and acceptance. Avoidance is accomplished by eliminating or entirely avoiding the risk. Of course, the best way to avoid an Internet computer virus risk is to not access the Internet. While this is generally not possible or realistic, the next most reasonable approach is to implement a correction. The correction may be to maintain current anti-virus software, utilize a personal firewall and implement a policy to not open emails and email attachments from individuals that are not known to the recipient.

Transference is accomplished by transferring the risk to a third party. Car, home and flood insurance policies are purchased for the purpose of transferring risk to the insurance company. Acceptance of the risk is a strategy where the cost of the risk is considered and compared to the benefit of the solution. If accepting the risk is less risky or less costly than the necessary solution then accepting the risk may a reasonable decision. An example of risk acceptance is when an organization decides to self-insure and does not purchase third party insurance.

With these four risk strategies for mitigating and managing risk in mind, the NP agency will begin the risk analysis phase. In this phase the organization will describe and prioritize all services performed (See Table 2), prepare an inventory of assets (See Table 3), prioritize disasters and threats based on historical information (See Table 4), estimate the likelihood of the threat occurrence (See Table 5), and assess the impact to the organization if the disaster occurs (See Table 6). Each item will be prioritized by assigning a level of importance using a scale of one to ten with ten signifying the greatest importance and one the least importance. While the priority contribution is a subjective scale, assigning relative significance can differentiate the importance of items. Participants must be cautioned from assigning high scores to each item**.**

Service	Description	Priority Contribution
Food Service	Prepare in the kitchen food to the elderly	10
Food Service	Deliver food to the elderly	9
Food Service	Prepare food for after school children	8

Scale: 1-10 – with 10 most important

Table 2: Services Performed

Assets

Assets are items of value to the organization. Assets may be grouped into categories for simplification. Table 3 below provides sample format and sample content information for clarification of possible assets.

Asset Inventory	**Description**	**Priority Contribution – Criticality**
Perishable Foods	All food refrigerated and other perishable foods in the kitchen	7
Computer Data	Contain client names, vendor names, accounting information, other	6
Kitchen Appliances (refrigerators, freezers stores, pots/pans)	Refrigerators, freezers, pots/pans, utensils	8
Building	Kitchen and Day care center	9
Delivery Vehicles	Cars, Vans, Trucks	5
Employees	Cooks, delivery, accounting	10

Scale: 1-10 – with 10 most important

Table 3: Assets

Other key assets to consider that were not provided in the sample table above may include cash, payroll accounting system, data and data backups, computer network, electricity, cell and land line phones, fax machines, donors, corporate partners, suppliers, volunteers and other assets required to maintain a fully functional NP organization.

Threats

The next step in risk analysis is to identify likely threats based on historical information and anticipated future occurrences. A threat is described as an impending danger or harm and can result in an undesired event. Threats are grouped into four categories including human, forces of nature, infrastructure and technology. In utilizing these categories to complete this section of the continuity plan individuals and teams will be able to focus planning toward the most likely specific threat occurrences. While 9/11, the East coast power outage, the 2005 hurricanes Rita and Katrina and the 2007 hurricane Dean may come to mind first, it is important to remember that natural disasters represent approximately only one percent of all serious interruptions (Nemzow, 1997). Though their impact may be the greatest, their likelihood is lowest. The threat of a loss of electricity is more likely a very real threat and one that should be on the threat list of every NP organization. Table 4 below provides a framework and sample content information for clarification of possible threats.

Threat Source	**Threat**	**Asset**	**Service/Group Affected**
Force of Nature (tree fell on power line	Loss of Electricity	Perishable Foods	Child Care – After School and Meals for

during strong winds)			the Elderly
Human	Important files deleted on the computer system	Computer Data	All NP Staff and customers
Human (spark from welder caused fire in building	Fire	Kitchen Appliances (refrigerators, freezers stores, pots/pans)	Kitchen staff and clients
Infrastructure Outdated	Flood (Broken Pipe)	Building	All NP Employees at specific location
Human – Deliberate	Physical Vandalism	Delivery Vehicles	Truck Drivers and elderly waiting on meals

Table 4: Threat Identification

Once services, assets and threats are identified the actual analysis can begin. The items in Tables 2 through 4 are used to import data into a threat to asset likelihood analysis (See Table 5) and a threat to asset impact analysis review (See Table 6). The organization will use the threats and assets identified in Table 3 and the information in Table 4, in conjunction with the experience and knowledge of the staff to assign the likelihood of occurrence in Table 5. The purpose of this table is to provide a master table that identifies the threats, assets and the likelihood of occurrence. The sample information is provided in Table 5 below.

Threat	**Asset**	**Likelihood of Occurrence**
Loss of Electricity	Perishable Foods	8
Important files deleted on the computer system	Computer Data	7
Fire	Kitchen Appliances (refrigerators, freezers stores, pots/pans)	5
Flood (Broken Pipe)	Building	4
Physical Vandalism	Delivery Vehicles	3

Scale: 1-10 – with 10 most likely

Table 5: Threats to Asset Likelihood

The impact of the threat to the asset is utilized to determine the severity of the threat. Again the expertise of the NP organization is used to assess and log assets and impact in Table 6.

Threat	**Asset**	**Impact**
Loss of Electricity	Perishable Foods	10
Important files deleted on the computer system	Computer Data	10
Fire	Kitchen Appliances (refrigerators, freezers stores,	10

	pots/pans)	
Flood (Broken Pipe)	Building	5
Physical Vandalism	Delivery Vehicles	4

Table 6: Threats to Asset Impact

Impact Analysis – Risk Prioritization – Step 3

The IA determines the impact of threats to the organization's assets and services. The IA table is built utilizing information from the multiple tables created in the risk analysis Step 2 phase. In Step 3, the IA objective is to prioritize how risk to the asset or service impacts the individual departments within the NP organization. For example, a threat that keeps the accounting department from being able to process payroll or pay vendor accounts payable will most likely be deemed a higher risk than a threat that keeps the staff from being able to print contracts for a short period of time. The table below utilizes the same threat and assets as utilized in prior tables. Then Criticality is utilized from Table 3, Likelihood from Table 5 and Impact from Table 6. The risk priority formula in Table 7 is: Risk Priority = Criticality + Likelihood + Impact. Risk priority is an important value in that it provides the organization with a numeric value that has been methodically derived through the various tables in Step 2. The risk priority indicates the area of resource focus and prioritization to be utilized when preparing for the most critical, likely disaster situations with the greatest potential impact.

Threat	**Asset/Service**	**Criticality**	**Likelihood**	**Impact Total**	**Risk Priority**
Loss of Electricity	Perishable Foods	7	8	10	26
Virus (from the Internet spread to all computers)	Computers	6	6	8	20
Fire	Kitchen Appliances (refrigerators, freezers stores, pots/pans)	8	5	10	22
Flood (Broken Pipe)	Building	9	4	5	15
Physical Vandalism	Delivery Vehicles	5	3	4	12
Bird Flu	Employees	10	1	5	16

Table 7: Business Impact Analysis – Risk Prioritization

Emergency Response Planning – Step 4

The Emergency Response Plan (ERP) documents preparation for events that threaten the safety and security of the organization's assets, operational functions and resources. The ERP defines the action steps to be taken while the emergency or disaster is in progress. The most important questions for an ERP plan are: what do I do now; who do I contact; what do I document and on what forms?

Independent of the size of the NP organization it is critical to have an Emergency Response Team (ERT) or an Emergency Response Individual (ERI) in the case of smaller operations. The ERT will include staff members, department heads and front line individual contributors that are intimately familiar with the responsibilities of the organization. The function of the ERP team is to create the ERP plan, test and maintain the plan and enact the plan in the event of an emergency.

In order to determine who should be on the ERT, the prior tables in Step 2 can be utilized as a reminder of expertise utilized to perform the services, the individuals most familiar with the assets and possibly individuals that have had prior emergency or disaster training. Emergency response roles for board members and volunteers should be included due to the relative importance of both groups in NP organizations. A sample of the team list is provided in Table 8.

Name	**Department**	**Responsibilities**	**Contact Information**
John Doe	Payroll	Collect time sheets and create bi-weekly payroll	Telephone number, e-mail and address
Mary Smith	Food Services	Prepare food for the elderly and after children care	Telephone number, e-mail and address
Henry Retz	Building Services	Contact to building utilities companies, electrical shut off, building water systems	Telephone number, e-mail and address
Tom Jones	Transportation	Deliver food to the elderly	Telephone number, e-mail and address
Betsy Jones	Public Affairs	Communicate with the new media	Telephone number, e-mail and address
Elizabeth Grace	IT	Computers, computer systems, phone lines, back-up copies of data, remote data copies, others	Telephone number, e-mail and address

Table 8 – Emergency Response Team List

Organizational Resumption Planning – Step 5

The next step is for the organization to resume offering services as soon as possible even if they may be offered in a different location or on a smaller scale. The Organizational Resumption Plan (ORP) focuses on how to recreate and maintain essential processes. The ORP provides procedures for recovering operations during or immediately following a disaster. These processes may possibly be at a remote location and at a time when normal operations and processes are not available. The organizational resumption plan will include many of the detailed responses to the questions below:

(1) Under what situations and under who's authority will the business relocate to another location?
(2) Is there another organization that can provide reciprocity of assistance such as facilities, equipment, personnel, communications capabilities or supplies?
(3) What are the vendors, partners, or secondary locations to consider when the primary location is no longer available?
(4) Under what situation and who's authority will the organization relocate back to the primary location?
(5) What scheduling must be completed before moving back to the primary location?
    a. Building renovation
    b. Utilities
    c. Employee moves
    d. Testing of facilities and systems
    e. Equipment relocation and set-up

Testing & Auditing – Step 6

While the plan may be well constructed and documented on paper, it is important to test the plan with either a simulated or real-life situation. As a general rule, all continuity plans should be tested annually and more often if there are changes in the services, systems, employees, processes and procedures. Testing of the plan can be accomplished in a variety of methods. One process that could be used is known as a table top exercise (Harris, 2005) where individuals discuss a hypothetical disaster and the necessary disaster recovery process and procedures. On the other extreme, hot site testing can occur where systems are actually taken off line, primary electrical sources are turned off and back-up electricity sources are brought on line in an attempt to create the issues that will occur during the disaster situation. Other testing methods that can be used are warm and cold site testing which include more testing steps than the table top and less testing details than the hot site testing discussed.

Plan Maintenance – Step 7

The final step of plan maintenance, is as important as creating the plan. Maintaining a plan with current and accurate information on assets, employee contacts, vendor contacts, up to date insurance plan information and coverage, test results and enhancements is mission critical. While it is easy to simply say "yes we have a plan" and check it off the list, a grossly outdated plan is like having no plan. Upon completion of the seven planning steps the organization can review the Readiness Index score to identify future work to improve continuity and disaster preparedness.

CONCLUSION

With 96% of the NP managers surveyed indicating continuity planning and training is needed, it is evident that these managers recognize the importance of the continuity planning and training process. This 7-step straight-forward approach to continuity and disaster recovery planning makes it possible for NP organizations to determine their organizational readiness and create a plan that improves the organization effectiveness in times of disaster. The NP organization that is prepared and ready for a disaster is better positioned to provide critical support to clients in need. The community capacity to protect its' citizens is increased when it is comprised of NP organizations that have implemented the 7-step business continuity planning process.

ACKNOWLEDGEMENT

The authors of this paper would like to extend a thank you to the University of Dallas, Spring, 2007 Graduate Information Assurance (IA) Capstone class for their work on this IA project. The team members included; Kimberly Reed, Lynh Le and Chris Petta. This project was in funded in part through a M. R. & Evelyn Hudson Foundation grant.

REFERENCE LIST

Blanke, S., McGrady, E. (2007). How to keep going when the going gets tough; Nonprofit continuity planning in preparation for organizational disruption. *Conference Proceedings of the International Academy of Business and Public Administration Discipline. 4*(2), 306-316.

Harris, S. (2005). *CISSP Exam Guide*. New York: McGraw-Hill/Osborne.

Meyer-Emerick, N., & Momen, M. (2003). Continuity planning for nonprofits. *Nonprofit Management and Leadership. 14*(1): 67-77.

Nemzow, M. (1997). Business continuity planning. *International Journal of Network Management, 7*, 127-136.

Robinson, M. (2003). *Disaster Recovery Planning for Nonprofits*. Lanham Maryland: Hamilton Books.

Wells, A., Walker, C., & Walker, T. (2007). *Disaster Recovery Principles and Practices*. Upper Saddle River NJ: Prentice Hall.

Whitman, M., Mattord, H. (2007). *Principles of Incident response and Disaster Recovery*. Boston MA: Thomson Course Technology.