Twelve Best Practices to Mitigate Risk Through Continuity Planning and a Scorecard to Track Success

Elizabeth McGrady
Appalachian State University

Sandra J. Blanke
University of Dallas

This prescriptive research describes a continuity planning readiness scorecard based on twelve best practices that can be used by organizations to focus planning, compare readiness with peers and track internal progress. The study of a sample of community organizations revealed that 58% of respondents had a continuity plan but most did not comply with all of the best practices. These findings assist in defining continuity readiness and suggest additional guidance to strengthen the readiness of organizations and communities in response to incidents, hazards and disasters. Training needs are also identified.

INTRODUCTION

The collaboration of community organizations including human service, health care, and public service is critical to effective community response to disasters. The heroic outpouring of assistance of community organizations in response to disasters has been well documented. While expectations of help are often exceeded (Homeland Security Institute, 2006) the question remains – how prepared are community organizations to ensure their continuity during a disaster or incident so that they are available to serve clients and support each other during and after a disaster? The purpose of this study was to:

1. Identify continuity and disaster response best practices.
2. Assess the continuity and disaster response readiness and vulnerabilities of community nonprofit organizations compared to the best practices.
3. Identify training needs.
4. Assess the ability of organizations to get help from or give help to other organizations.
5. Construct a scorecard that enables organizations to track progress of the organization and key collaborators in continuity planning.

Community organizations hold unique and important roles in disaster response by serving the needs of victims as first responders, repositories and distributors of monetary and in-kind donations, and sheltering, feeding, and clothing victims (Robinson, 2003, Brudney & Gazley, 2009). Fundamental to the success of disaster response is the ability of individual organizations to deliver on promised services (Provan, Veazie, Staten, & Teufel-Shone, 2005). Disaster response requires a community-wide collaborative effort and a chain can only be as strong as the weakest link. A first step is individual organization continuity planning.

Readiness Status

Completion of continuity plans improves organizational resiliency (Sommer, 2009). However, government reports such as the Department of Homeland Security Office of Inspector General (2006) and A Performance Review of FEMA's Disaster Management Activities in Response to Hurricane Katrina (2006) have indicated community organizations are not adequately prepared to respond to disasters.

In a study of the Katrina response by the Chicago Public Health Department the participating community organizations reported lack of planning as their number one deficiency (Broz, Levin, Mucha, Pelzel, Wong, Persky, & Hershow, 2009). While many organizations have at least a rudimentary continuity plan in place (see Table 1) only half had tested the plans (Strategic Direction, 2008). This compares with the study of Mayer, Moss, & Dale (2008) where only 39.3% of businesses reported completing "many" preparedness activities and 46.1% "some".

TABLE 1
ORGANIZATIONS COMPLETING AT LEAST SOME PLANNING

Study	Organizations with at least some continuity planning
Clas, 2008	69%
Strategic Direction, 2008	50%
Mayer, Moss, & Dale, 2008	85%

Best Practices

Community organizations often have limited resources and typically devote those resources to patient, resident and client needs. Continuity planning must be simple and focused for this sector. This study identifies twelve best practices in continuity planning using a compilation of source material including the FEMA Emergency Management Guide (FEMA, 2001), National Institute of Standards and Technology (NIST) (Swanson, Wohl, Pope, Grance, Hash, & Thomas, 2002), the U.S. Department of Homeland Security National Preparedness Guidance (2005) in addition to numerous articles and studies (Wong, Monaco, & Sellaro 1994, Semer 1998, Harrald & Lee, 1999, Bandyopadhyay, 2001, Rike, 2003, Robinson, 2003, Meyer-Emerick & Momem, 2003, Harris, 2008, Blanke & McGrady, 2008). Based on our review the following were identified as best practices:

1. Identification of threats to the organization - A threat is described as an impending danger or harm that can result in an undesired event. Threats are grouped into four categories including human, forces of nature, infrastructure and technology.
2. Assigning probability of the threat occurring - This step focuses planning toward the most likely specific threat occurrences. Natural disasters represent approximately only one percent of all serious interruptions. Though their impact may be the greatest, their likelihood is lowest.
3. Identification of organizational vulnerabilities – Vulnerabilities include loss of resources, assets, financing, funding, cash flow, ability to communicate, availability of human resources, facilities, supplies, files, data and information.
4. Evaluation of potential impact of vulnerabilities – This practice describes the impact on the organization and operations if assets are compromised or lost.
5. Having a plan and annual review of the plan – Not only should an organization have a plan but it should be reviewed at least annually.

6. Updating the plan annually - Plan maintenance is as important as creating the plan, a grossly outdated plan is like having no plan. This includes key contact information.
7. Testing the plan annually - Although 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 frequently if there are changes in the services, systems, employees, processes and procedures. Testing of the plan can be accomplished using a variety of methods including hypothetical exercises.
8. Listing key contacts in the plan – The plan should include current and accurate information on assets, employee contacts, vendor contacts, up-to-date insurance plan information and coverage, patient or client information, continuity collaborators, volunteers, members of the governance board, and media contacts. It may include donors if the organization is dependent on contributions for funding.
9. Electronic copy storage – Continuity plans may be destroyed by disasters such as fire or flooding. The plan information needs to be available at any time and at off-site locations.
10. Alternate location to operate – The plan should describe how and where services can be delivered in the event of a loss of the facility.
11. Service repair contracts – A list of the vendors under contract to restore key assets or services. Once again this should be available electronically.
12. Communicating the plan with other organizations – Do the organization's partners and collaborators know of the organization's plans, is there an agreement in writing, how they will be contacted and in what circumstance, what is the relationship with Emergency Management (EM)?

METHODOLOGY

To address the research questions we developed a survey based on the best practices identified. We then used the items to evaluate the readiness and level of continuity planning of Dallas, Texas area community and public sector organizations. Open-ended questions were developed to identify specific vulnerabilities and training needs. A panel of ten representatives from the community and public service sectors tested the assessment and reviewed the instrument instructions and questions for clarity, understandability and ease of use. The assessment was conducted using senior managers of the members of the Community Council of Greater Dallas (2007). CCGD is a cross-sector coalition of human service, legal aid, health care, educational and public service organizations.

We created the Readiness Index by converting the information found in the study to a scale that could serve as a scorecard. The twelve best practices items were used to construct a Readiness Index by tabulating affirmative responses of level of completing the practice. Each item accomplished was scored one point and the total possible Readiness Index score was fourteen.

Indexes can be used in a variety of ways. They can be constructed to quantify multiple pieces of information into a single number to provide a meaningful but simple indicator. Examples of indexes include the Social Vulnerability Index which uses wealth, age of structure, density of the built environment, occupant data and infrastructure dependence of inhabitants to predict social vulnerability as a result of disaster-related outcomes (Myers, Slack, & Singlemann, 2008). Adrianto and Matsuda (2004) constructed a Composite Vulnerability Index by weighting then adding economic exposure, economic remoteness, and the economic impact of disasters. Vulnerability increased with the weighted higher incidence of each. The Construction Industry Institute used best practices to construct a security-rating index (SRI) to measure levels of incorporation of security practices (Marshall, Chapman, & Leng, 2004). A simple index scale developed by Roberto, Bohmer, Richard, and Edmondson (2006) uses additive responses to a Likert scale to six questions as a diagnostic tool to quickly determine an organization's preparedness for ambiguous threats. This scale was used as a basis for our Readiness Index.

ANALYSIS

Readiness

Fifty-eight per cent of respondents reported they had a disaster recovery plan in place, while 42% did not. Though respondents stated they had constructed a plan not all best practice items were completed. Only 16.7% had reviewed, updated, and tested the plan in the last year. A Readiness Index was compiled by averaging the number of best practices completed. Table 2 lists the items included in the Readiness Index and the percentage of organizations that reported completing each factor in the past year. The mean score for the Readiness Index was 4.79 (sd= 2.83) out of the possible score of 12.

TABLE 2
PERCENTAGE OF ORGANIZATIONS COMPLETING READINESS INDEX ITEMS

Index Items	% Yes
Key contact list	71.2
Repair and service contract	69.7
Reviewed plan in past year	51.5
Identified vulnerabilities	47.0
Alternate location to operate	36.4
Updated plan in past year	36.4
Communication plan with reciprocal agencies	36.4
Electronic copy of plan stored	31.8
Identified threats	28.8
Identified vulnerabilities plus impact	28.8
Identified threats with probabilities	24.2
Tested plan in past year	16.7

Vulnerabilities and Impact

Respondents were asked if they had experienced a disaster using an open-ended question, and if so, what was their top-of-mind greatest vulnerability or area of concern. Fifty-two per cent had experienced a disaster of some type. The most frequently reported vulnerability items were funding, finances or cash flow (30.8%) and the inability to communicate (30.8%). Human resources availability (including volunteers) and facility and utilities were both reported by 11.5% of respondents. Security and safety issues were the greatest concern of 7.7% of respondents and availability of supplies and data or files were the top concerns of 3.8%.

Respondents were asked to select from a list which specific resources would cause significant immediate impact to the organization's ability to operate if unavailable or impaired. The resources with the greatest immediate impact if lost were staff (46%), electricity (46%), cell phones (40%), water (40%), telephones (38%), and information systems (34%). Respondents were asked the magnitude of loss impact of specific resources (ranging from very low to very high). Resources that at least two thirds of the respondents reported as having very high impact on the inability of the organization to function if unavailable or impaired were donors, clients, computers and computer networks, data, and electricity.

Training and Preparation Needs

Ninety-six per cent of respondents agreed they needed disaster preparation training. The greatest need reported was overall planning and training assistance. Specific items identified were training or planning for preparation to ensure continuity of communications during a disaster, development of plans, ability to coordinate and link with other organizations, finding resources, prioritizing actions internally, and evacuation and relocation. (See Table 3).

TABLE 3
LIST OF TRAINING AND PLANNING NEEDS

	%
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

Reciprocity and Availability of Help

In the event of a disaster 42% of respondents reported that there was another agency that could temporarily support their services. A slightly larger number (52%) reported they could temporarily help another organization within their current staffing levels. In addition, 42% reported that they could increase their staffing levels if needed in response to a disaster. Organizations with a higher overall Readiness Index reported they were more likely to be able to support others in times of disaster implying better compliance with the best practices could improve community collaboration and reciprocity. Two best practices predicted a greater likely hood of being able to help others in time of disaster - having repair and service contracts and having a key contact list. Almost half replied their organizations could not identify a resource to help with continuity and disaster recovery training and planning.

The Compliance Scorecard

A scorecard utilizing the readiness index items was developed to serve as an internal and external benchmark organizations can use to compare their continuity readiness with peer organizations and to track progress in planning improvement. The compliance scorecard (See Table 4) indicates not only the

TABLE 4
CONTINUITY PLANNING COMPLIANCE SCORECARDS

Item	0	+1	+2	Score
Threats	Not identified	Identified	Identified and assigned probability	
Vulnerabilities	Not identified	Identified	Identified and forecast impact	
Written plan	Do not have	Have	Have and review annually	
Plan testing	Do not test	Test annually	Test and revise annually	
Key contacts	Do not have list	Have identified and listed	Have list stored remotely or electronically	
Alternate location to operate	No alternate location	Identified alternate location	Have alternate location with written agreement	
Interoperability	Have not communicated with other organizations	Have communicated plan with other organizations	Have written organization interoperability	
			Total Score	

completion of each of the seven practices but also a degree of compliance which includes all 12 best practices. Level of compliance can be indicated using dashboard indicators of red (non-compliant), yellow (partially compliant) and green (fully compliant) for easy visual tracking of progress.

IMPLICATIONS

Though the primary mission of community organizations will always be serving client needs, organizations must devote time and resources to ensuring their continuity. No survival – no mission fulfillment. This study found that almost half of community organizations do not have continuity plans though these are the very organizations communities rely upon in times of disaster. Even organizations that stated they had plans in place are not ready to the level of rigor recommended by experts. The study identified a clear list of best practices in continuity preparedness and a means for organizations to assess needs, gaps and progress. With ninety-six percent of the organizations participating in this study reporting they need some form of training and plan development assistance it remains a senior management and community priority, even in a time of diminished resources.

Continuity planning begins as a strategic imperative. Allocation of resources to planning, training, risk mitigation and ongoing maintenance of the continuity plan requires ongoing commitment. Organizations that must meet the requirements of external bodies or regulations such as state licensure, accreditation, certification, HIPPA, or the Graham Leach Bliley Act must maintain this strategic commitment to continuous quality improvement. A simple scorecard of best practices can be used by individual organizations to ensure their ability to serve the community during disaster by increasing their own readiness. Continued requirements by regulatory and accrediting bodies will assist community organizations in prioritizing both planning and training. The Federal Emergency Management Administration and other organizations have developed free web-based material to assist with planning and preparation but an important first step is the recognition that your organization does not comply with best practices. This simple scorecard can assist those responsible for governance of organizations in evaluating continuity vulnerabilities and preparedness.

LIMITATIONS

We applied this scorecard to public service and community organizations who were members of CCGD. Although this sample contained a variety of organizational types, caution should be used before generalizing these results to other community and business entities.

REFERENCES

A performance review of FEMA’s disaster management activities in response to Hurricane Katrina. Retrieved on November 8, 2006, from [http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_06-32_Mar06.pdf]

Adrianto, L. & Matsuda, Y. (2004). Study on assessing economic vulnerability of small island regions. *Environment, Development and Sustainability,* ABI/INFORM Global, 6(3), 317-336.

Bandyopadhyay, K. (2001). The role of business impact analysis and testing in disaster recovery planning by health maintenance organizations. *Hospital Topics*, 79(1), 16-22.

Blanke, S. & McGrady, E. (2008). A performance-based approach to continuity planning. In James Langabeer (Ed.) *Performance Improvement in Hospitals and Health Systems*. Health Information and Management Systems Society.

Broz, D, Levin, E, Mucha, A, Pelzel, D, Wong, W, Persky, V, & Hershow, R. (2009). Lesson learned from Chicago’s emergency response to mass evacuations caused by Hurricane Katrina. *American Journal of Public Health,* 99(8), 1496-1504.

Brudney, J, & Gazley, B. (2009). Planning to be prepared: An empirical examination of the role of nonprofit organizations in county government emergency planning. *Public Performance & Management Review*, 32(3), 372-399.

Community Council of Greater Dallas Web Site mission statement, Retrieved on February 8, 2007, from [http://www.ccgd.org/]

Department of Homeland Security Office of Inspector General. (February 2006). The federal response to Hurricane Katrina lessons learned. Retrieved on February 10, 2007 from [http://www.whitehouse.gov/reprots/katrinalessons-learned/]

Federal Emergency Management Agency (FEMA). *Emergency Management Guide for Business and Industry.* 2001 [http://fema.gov/library/bizindex]

Harrald, J, & Lee, Y. (1999). Critical issue for business area impact analysis in business crisis management: analytical capability. *Disaster Prevention and Management*. Bradford, 8(3), 184.

Harris, S. *CISSP Exam Guide*. New York: McGraw-Hill/Osborne. 2008.

Homeland Security Institute (2006). *Heralding unheard voices: The role of faith-based organizations and nonpublic service organizations during disasters.* Arlington, VA: Department of Homeland Security Science and Technology Directorate.

Marshall, H, Chapman, R, & Leng, C. (2004). Risk mitigation plan for optimizing protection of constructed facilities. *Cost Engineering.* Morgantown, 46(8), 26-33.

Mayer, B, Moss, J, & Dale, K. (2008). Disaster and preparedness: Lessons from hurricane Rita. *Journal of Contingencies and Crisis Management.* 16(1), 14-23.

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

Myers, C, Slack, T, & Singlemann, J. (2008). Social vulnerability and migration in the wake of disaster: the case of Hurricanes Katrina and Rita. *Population Environment*, 29, 271-201.

Provan, K, Veazie, M, Staten, L, & Teufel-Shone, N. (2005). The use of network analysis to strengthen community partnerships. *Public Administration Review*, 65(5), 603-613.

Rike, B. (2003). BIA best practices – prepared or not… that is the vital question. *Information Management Journal*, Lenexa, 37(3), 25-27.

Roberto, M., Bohmer, R, & Edmondson, A. (2006). Facing ambiguous threats. *Harvard Business Review,* 84(11), 106-113.

Robinson, M. *Disaster recovery planning for nonprofits*. Lanham Maryland: Hamilton Books. 2003.

Semer, L. (1998). Disaster recovery planning. *The Internal Auditor*. Altamonte Springs, 55(6), 40-46.

Sommers, S. (2009). Measuring resilience potential: an adaptive strategy for organizational crisis planning. *Journal of Contingencies and Crisis Management,* 17(1), 12-23.

Strategic Direction. (2008). Plan for disaster before it happens; Do organizations know how to manage a crisis? Bradford, 24(3), 6.

Swanson, M., Wohl, A, Pope, L, Grance, T, Hash, J, & Thomas, R. (2002). Contingency planning guide for information technology systems. National Institute of Standards and Technology Special Publication 800-34. [http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf]

Wong, B, Monaco, J, & Sellaro, C. (1994). Disaster recovery planning: suggestions to top management and information systems managers. *Journal of Systems Management*. Cleveland, 45(5), 28-32.

U.S. Department of Homeland Security National Preparedness Guidance (2005) [http://www.ojp.usdoj.gov/odp/docs/NationalPreparednessGuidance.pdf]

TABLE 1
ORGANIZATIONS COMPLETING AT LEAST SOME CONTINUITY PLANNING

Study	**Organizations with at least some continuity planning**
Clas, 2008	69%
Strategic Direction, 2008	50%
Mayer, Moss, & Dale, 2008 (business)	85%

TABLE 2
PERCENTAGE OF ORGANIZATIONS COMPLETING READINESS INDEX ITEMS IN PAST YEAR

Index Items	**% Yes**
Key contact list	71.2
Repair and service contract	69.7
Reviewed plan in past year	51.5
Identified vulnerabilities	47.0
Alternate location to operate	36.4
Updated plan in past year	36.4
Communication plan with reciprocal agencies	36.4
Electronic copy of plan stored	31.8
Identified threats	28.8
Identified vulnerabilities plus impact	28.8
Identified threats with probabilities	24.2
Tested plan in past year	16.7

N=66

TABLE 3
LIST OF TRAINING AND PLANNING 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

TABLE 4
CONTINUITY PLANNING COMPLIANCE SCORECARD

Item	0	+1	+2	Score
Threats	Not identified	Identified	Identified and assigned probability	
Vulnerabilities	Not identified	Identified	Identified and forecast impact	
Written plan	Do not have	Have	Have and review annually	
Plan testing	Do not test	Test annually	Test and revise annually	
Key contacts	Do not have list	Have identified and listed	Have list stored remotely or electronically	
Alternate location to operate	No alternate location	Identified alternate location	Have alternate location with written agreement	
Interoperability	Have not communicated with other organizations	Have communicated plan with other organizations	Have written organization interoperability	
			Total Score	