



2010

The impact of people continuity on organizational resilience



Personal Recovery Concepts

All rights reserved.

Copyright March, 2010

Introduction

Risk management practices have fundamentally changed

Threats to the nation's safety and economy have proliferated as the global footprint of firms expands. Beyond weather phenomena, firms are at risk for terrorism aimed at their IT infrastructures, facilities and people, and from turbulent geo-politics. Other crises stem from internal cyber, financial, safety and environmental controls. These threats become extended throughout a firm's supply chain. The changing landscape has made doing business – well, risky.

Whereas risk management was an independent activity embedded within an organization, agency, community or household, the interdependent impact that a crisis has on the entire socio-economic system has driven fundamental shifts in how these risks must be managed. At their core is the role business plays in restoring the economic foundation of an affected region.

Therefore, fundamental shifts in an organization's risk management practices include:

- From independent risk management to a shared responsibility for preparedness
- From operational readiness to organizational resilience
- From operationally focused plans to plans that include the resilience of people
- From a burden of responsibility on the business continuity manager to the C-suite

Standards that shape a culture of preparedness have evolved to address these shifts in risk management practices. Both the shift and how standards support them are detailed below.

Preparedness is a shared responsibility

The first fundamental shift is that preparedness is recognized as a shared responsibility because the behavior of any entity in a crisis has an interdependent impact on the whole.

Secretary Janet Napolitano states: *"Preparedness is a shared responsibility and everyone—including businesses, universities and non-profit organizations—has a role to play. Ensuring our private sector partners have the information and training they need to respond to disasters will strengthen our efforts to build a culture of preparedness nationwide."*

Napolitano supported that call to action with newly proposed standards for the private sector titled PS-Prep. *These standards were developed by the National Fire Protection Association, the British Standards Institution and the ASIS International, and were selected based on their scalability, balance of interest and relevance to PS-Prep¹.*

¹ Secretary Napolitano Announces New Proposed Standards for Private Sector Preparedness, DHS Press Release, October 15, 2009

Operational readiness has moved to organizational resilience

Given the impact 9-11 and Hurricane Katrina had on their regions, the emphasis most directly following these catastrophic events was on readiness. Readiness was defined as preparedness to respond during an emergency, focused on the protection of life and physical assets. Organizational plans centered operationally on having critical infrastructure systems back online as quickly as possible.

As reports emerged, not just from extreme weather, but from ensuing catastrophes like the bombings in London, Bali and Madrid, Anthrax, SARS and H1N1, among the largest proven gaps in the readiness model became people. Not so far as in what roles and responsibilities they had in response efforts, but in their own personal preparedness that ensured the self-reliance of their families and loved ones so they were available more quickly and with better focus to the organizations that relied on them.

Moreover, it was learned that being *ready* missed opportunities to plan for recovery, effectively delaying the rebuilding and restructuring of core businesses and thereby the economic vitality of the affected region.

As such, national guidelines have evolved from readiness to resilience. Resilience is a more holistic approach to regional and economic recovery, as stated in the newest ASIS standards: *“The challenge goes beyond most emergency response plans or disaster management activities previously deployed. Organizations now must engage in a comprehensive and systematic process of prevention, preparedness, readiness, mitigation, response, continuity, and recovery. It is no longer enough to draft a response plan that anticipates disasters or emergency scenarios. Today’s threats require the creation of an on-going, dynamic, and interactive process that serves to assure the continuation of an organization’s core activities before, during, and – most importantly – after a major crisis event.”*²

Organizational resilience depends on the resilience of the people it relies on

An emphasis has been placed on personal preparedness of American families, promoted through lessons learned from major catastrophic events preceding 9-11 and Hurricane Katrina. However, the enormity of these latter events further underscored the weaknesses in America’s culture. These included a sense of complacency with our own safety; a reliance by citizens on the help of authorities in life-threatening situations; and an unrealistic expectation that our first-responders and critical business teams will be available and focused to support rescue or recovery when they themselves are victims of the same threat.

In fact, the entire spectrum of personal preparedness has proven to be the most critical gap in emergency plans for businesses, agencies, communities and families. For this reason, the Secretary and scores of other reports have moved the issue of personal preparedness to the forefront as one of our nation’s highest priorities to establishing a culture of readiness and resilience.

The evidence supports this conclusion. For example, the 2009 *Preparedness in America* study³ found that 60% of Americans who considered themselves prepared for an emergency expect to rely on emergency first responders in the first 72 hours following an emergency.

² ASIS SPC.1 2009, Annex A – American National Standard for Security

³ Personal Preparedness in America: Citizen Corps National Survey August 2009

Contrast that expectation to the reality stated in the 2007 Department of Homeland Security report that “As *uniformed emergency responders constitute less than one percent of the total U.S. population, it is clear that citizens must be better prepared, trained, and practiced on how best to take care of themselves and assist others in those first, crucial hours during and after a catastrophic incident.*”

For 70% of businesses who have developed robust business continuity and emergency response plans, only 25% have also accounted for human resiliency⁴. This fundamental gap has left businesses with robust plans, but with no one to execute them. In real-world situations, employee availability during and after a continuity event has proven to have a major impact to increased time-to-recovery and associated costs for a business. Even when employees do report for work, they lose substantial focus if they have not accounted for the safety and security of their family and their personal-recovery issues.

In an Executive Analysis Report on a Michigan-based fire department deployed to ground zero, it was noted, “*There is a difference between being ready “to go” and ready “to part”. Being ready “to go” means having our bag packed, all shots up to date, and other duty essential preparations completed. Being ready “to part” from your spouse and other family members means being aware of the personal and family issues related to separation, and being prepared to deal as constructively as possible with those issues.*”⁵

Beyond specific plans that ensure the safety and security of family members *during* an emergency, the largest impact to employee availability *after* an event is the restructuring of their life – from securing alternate shelter to the rebuilding of personal records. Because of previous emphasis on “readiness”, concern for what it would take after an event for an individual to recover was not expected in plans and its importance was not recognized or communicated. The *Preparedness in America*³ study found that among individuals, only 2% had stored financial documents in a restorable format or alternate location. Only 9% had recorded the names, dosage and frequency of the medications either they or family members took and only 1% had made any arrangements to copy and store personal identification.

How does personal preparedness impact organizational resilience? Consider that among an organization’s most critical assets is its data. The safeguards an organization makes to mirror its data, to have redundant servers and alternate offsite IT locations are key to the organization restoring operations.

At individual levels, the critical reliance on personal data to restoring their personal life is *exactly* the same. An individual who also experiences a catastrophe has financial and legal records, insurance and alternative shelter considerations and the need for medical information and personal identification in order to restore their personal affairs to pre-event conditions.

Identity theft is a correlated example because it too has a high-involvement with personal data. When a person is the victim of identity theft, the average time-to-recovery is 81 hours in absenteeism and lost productivity to the company. When the area a company and its employees work in is also devastated, multiple employees are impacted with partial or complete loss of such data, each having the same 81 hours to recover – **creating an exponential cost-impact to the organization caused directly by lack of personal preparedness.**

⁴ Forrester Research, Dec. 2006, Workforce Continuity – a Critical Strategy in your Business Continuity Plan - referenced in the Varolli Corporation Report, “*When the lights are on but nobody’s home.*”

⁵ Ohio Air National Guard, 2004

Whether the employee manages these personal issues during or after the event, the organization still absorbs the exponential impact of their personal recovery time and its own time-to-recovery is delayed.

The longer it takes an employee to be available to their employer, the higher the costs to the business escalate regardless of the steps the business had taken to establish backup systems. A Meta Group study indicates that the cost-per-hour for downtime across a broad range of industries ranges is in the millions of dollars⁶.

Industry Sector	Revenue/Hour	Revenue/Employee-Hour
Energy	\$2,817,846	\$569.20
Telecommunications	2,066,245	186.98
Manufacturing	1,610,654	134.24
Financial institutions	1,495,134	1,079.89
Information technology	1,344,461	184.03
Insurance	1,202,444	30.92
Retail	1,107,274	244.37
Pharmaceuticals	1,082,252	167.53
Banking	996,802	130.52
Food/beverage processing	804,192	153.10
Consumer products	785,719	127.98
Chemicals	704,101	194.53
Transportation	668,586	107.78
Utilities	643,250	380.94
Health care	636,030	142.58
Metals/natural resources	580,588	153.11
Professional services	532,510	99.59
Electronics	477,366	74.48
Construction and engineering	389,601	216.18
Media	340,432	119.74
Hospitality/Travel	330,654	38.62
Average	\$1,010,536	\$205.55

According to KPMG, 40 percent of companies that suffer a major business disruption go out of business within two years because they are unable to recover from the long-term effects of a crisis⁷.

In an emergency, the biggest deterrent to employee availability proved to be personal preparedness for unexpected events or emergencies. Where a personal and/or family plan was absent, employee availability and focus was significantly lower, contributing directly to increased time-to-availability for the organizations that relied on them.

Therefore, a direct and indelible link has proven to exist between the resilience an organization can achieve and the resilience of the people it relies on. In a 2004 Department of Defense report, the agency stated ***“The link between family and mission readiness is clear.”***

⁶ META Group, Inc., "Quantifying Performance Loss: IT Performance Engineering and Measurement Strategies", November 22, 2000

⁷ nFrame, "Computing the Cost of Downtime"; referenced in InterCep, "The Business Case for Preparedness", New York University, August 21, 2007

ASIS calls upon organizations to establish recovery-time objectives and priorities to include “resource management objectives for response times, personnel, equipment, training, facilities, funding, insurance, liability control, expert knowledge, materials and time frames within which they will be needed from organization’s resources and from any partner entities; and procedures for stakeholder assistance, communications, strategic alliances and mutual aid”.

“The organization shall ensure that any person(s) performing incident prevention, preparedness, and response measures on its behalf are competent on the basis of appropriate education, training or experience, and retain associated records”.

A shift of burden for risk management has moved from the business continuity manager to the C-suite.

Resilience has become a shareholder issue. According to a report jointly undertaken by Ernst & Young, Oxford Metrica and New World Research, “For Global 1000 firms, there is a high probability of a crisis resulting in substantial decline of stock price during any five year period. How management responds is “destiny determining” for both the company and its CEO.”

Its findings determined that when a sudden shift in shareholder value is precipitated by a crisis, the shareholder value gain or loss is sustained one year post-event. The shift in shareholder value is largely determined by the manner in which management overcomes the crisis before, during and after the event. While losses are recovered to some degree, the sustained loss continues to range from -20 to -40 percent. While losses can never exceed 100%, gains have no limit on the positive value they can add to the firm.

The shift in focus from readiness to resilience is in large measure a strategy to improve business survivability. Such catastrophes have proven the extraordinarily high rate of failure by businesses, with as many as 40% failing completely⁸. **The domino effect of failed businesses to people, infrastructure rebuilding and recovery becomes the determining factor in the holistic recovery of the region.**

ASIS further supports the impact of crisis management on the cost to the organization. It states: *When assessing impacts the organization should consider:*

- a) *Human cost: Physical and psychological harm to employees, customers, suppliers and other stakeholders.*
- b) *Financial cost:*
- c) *Corporate image cost:*
- d) *Economic losses to the community in which the organization operates*
- e) *Environmental impacts:*

⁸ nFrame, “Computing the Cost of Downtime”; referenced in InterCep, “The Business Case for Preparedness”, New York University, August 21, 2007

The difference between ready and resilient emergency planning

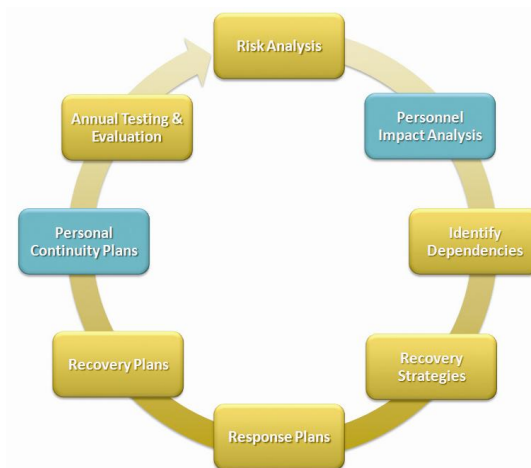
Ready means the organization has an alternate site location, redundant servers, data mirroring, evacuation plans, communication trees and other operationally focused plans. Ready means the organization has identified the key personnel who will execute its emergency response plan.

Resilience means the organization has considered people in its planning. It has conducted a personnel impact analysis that considers the demographics, culture and geography of its workforce as well as dependency, workplace and availability issues.

Its employees have addressed the highest priority they have in any threatening situation – the safety and security of their family and loved ones and a means to restore their critical life information. In so doing, the organization has significantly reduced the time it takes for employees to be available, focused and productive to the workplace so that the organization can resume revenue generating activities.

A resiliency based emergency planning model

Based on the known elements of continuity plans outlined to the right, there remains a gap for human resiliency. A resiliency based emergency planning model includes two new elements: ***A Personnel Impact Analysis*** uncovers critical facts that affect how an organization plans for people and their roles in emergency response and recovery. Validation of that preparedness needs to be included in the overall continuity plan and tested where appropriate. ***A Personal Continuity Plan*** prepares employees with the mechanism to develop and validate a personalized emergency plan based on their workplace and home-based responsibilities. A more appropriate model would include these components for critical team members. **This ensures they are available to fulfill their responsibilities faster and with greater focus** given the added confidence in the safety and security of their family and the pre-planning for their own personal recovery.



Basic components of continuity programs

1. Organizational policy on crisis management, business continuity or continuity of operations
2. Complete a risk analysis of your environment
3. Complete a business impact analysis or operational impact analysis for risks
4. Identify interdependencies (who counts on you and vice-versa)
5. Develop and assess recovery strategies
6. Develop a resumption plan
 - a. Sign-off or approvals
7. Develop a response plan/incident management plan
8. Develop a communications/notifications system or process
9. Test, test, test
10. Evaluate and validate the overall program
 - a. Reporting
 - b. Program maturity analysis

Summary

In the past, risk management focused almost entirely on operations with emphasis on safety and resumption of operations during a continuity event. Over time, this focus has proven to leave companies with little or no plans for recovery *after* an event, increasing the financial impact and the likelihood of business failure. The net impact of business failure was that an affected region was far slower to recover.

All risk management plans – whether housed in a business, agency of first-responders or community support agencies – relied on a single common asset: people. Yet conventional approaches to continuity plans assumed people would be available to execute the plans that had been made and practiced. In testing scenarios, employees were available to execute the plan with no concern for the safety and security of their own families. In this scenario, testing provides a false-positive. Under actual emergencies where the people the organization relied on most were also victims of the disaster, a lack of personal preparedness by employees diminished employee availability and focus, effectively increasing time-to-recovery and the associated costs an organization incurred. The domino effect on the organization proved insurmountable for as many as 40 percent of businesses that failed within two years following a catastrophic event.

Therefore, the “link between family preparedness and mission readiness is clear”. Business planning practices have evolved to include the resilience of people, including critical infrastructure, societal assets and the impact of cultural heritage. The improved planning models include a personnel impact analysis and implementation of personal continuity plans for employees. This model works to ensure the individuals an organization relies on have prepared beforehand not only for the safety and security of their family and loved ones during an event, but also for their expedient recovery after an event – thereby increasing their availability to the organization and reducing the financial impact to an organization’s time-to-recovery.

The business of risk management has naturally moved up to the C-suite as a priority and the tenets of risk management have changed as conventional wisdom is tested and adjusted based on lessons learned. Specifically, a correlation has been made between the manner in which an organization manages a crisis and shareholder value. The negative or positive impact to shareholder value is “destiny determining” in that its impact is sustained one year post-event.

Personal Recovery Concepts

Personal Recovery Concepts are specialists in people continuity. Its training and tools are designed to help organizations create a prepared workforce. In so doing, the company will reduce the costs related to everyday workforce disruptions, while mitigating the most common documented gap during natural disasters: employee availability and focus.

Personnel Impact Analysis

A personnel impact analysis uncovers critical facts that affect how an organization plans for people and their roles in emergency response and recovery.

A personnel impact analysis is conducted using an Employee Preparedness Survey (EPS).

The EPS is a 25-30 item survey questionnaire that is customized specific to the organization. It is a web-based instrument that takes 5-10 minutes to administer and complete.

The EPS analyzes four categories:

- Demographics
- Work responsibilities
- Availability issues
- Dependency issues

The survey data is aggregated to protect individual information and is analyzed to identify areas of personnel vulnerability.

Areas of concern are addressed in emergency response and recovery plans and are used to customize the personal continuity training.

Personal Continuity Plan

A personal continuity plan increases employee availability by preparing employees and their families to cope with the types of emergencies your organization must grapple with. It has the added benefit of preparing employees for everyday personal emergencies that sap organizations of \$268 billion in profits and productivity every year – such as home fires, identity theft, elder- and child-care and unexpected death. By preparing individuals at a personal level, your organization mitigates the exponential impact an unprepared workforce has during a crisis.

Personal Recovery Concepts' delivers a structured qualification system that drives individual preparedness and a measurable outcome for the sponsoring organization. The program benefits organizations by assisting employees to create personalized family and workplace continuity plans that make them ready and resilient. Completion of the program earns the employee a signed Personal Continuity Certificate – endorsed by Personal

Recovery Concepts and the SOLE – the International Society of Logistics – that can be recorded by human resources and provides organizations a competitive advantage.

Individual preparedness has fundamental similarities across community, business and government. Where it differs, Personal Recovery Concepts' Complete solution is customizable to an organization or agency's specific needs.

It is the only customizable program that includes a software-based mechanism to help employees build a personal continuity plan specific to their workplace and home-based roles and responsibilities.

About Personal Recovery Concepts

Personal Recovery Concepts, LLC is a leader in the sector of people-continuity services for government, business and consumers with offices in Huntington Beach, California and Harrison Township, Michigan. Its products and services focus on increasing employee availability by simplifying the information needed to recover from a wide array of loss or emergencies, organizing this information in simple, highly restorable formats, and preparing individuals through risk assessment, developing a family emergency plan and the prevention, preparation and recovery from commonly occurring emergencies to natural disasters. Personal Recovery Concepts' Complete Solution solves the gap in human resiliency for government first-responders, business critical response teams and for employees who face everyday loss with a realized cost impact to the businesses they work for.

www.personalrecoveryconcepts.com

866-528-9186.