The International Emergency Management Society
9th Annual Conference Proceedings
University of Waterloo, Canada, May 14-17, 2002

HOW TO DESIGN, DEVELOP AND IMPLEMENT A SUCCESSFUL BUSINESS CONTINUITY PROGRAM

Geary W. Sikich

Principal, Logical Management Systems, Corp.

Key Words: Crisis, Continuity, Planning, Hazard, Vulnerability

Abstract

Most organizations plan for business success. Yet, few plan for the potentially devastating effects of an event that becomes a crisis. Crises can take many forms; being prepared can be the most effective tool you can employ to assure the survivability of your business.

Connectivity, Speed and Intangible Values are the new driving forces in business today. Traditional business boundaries are blurring as everyone becomes electronically connected. The traditional rules governing the conduct of business are blurred as businesses are redefined, products become services, services become products and business lines change constantly.

As business change accelerates, it is getting more and more difficult for traditional strategists to achieve an accurate focus on the current situation. Strategy, in the traditional sense, is outdated before it can be implemented. Speed, operating at real time, is pushing traditional strategy development, forecasting, competitive intelligence collection and analysis to new limits. For every organization vision, mission and values are important. They shape strategy for the organization. Strategy in turn, is influenced by information in the form of competitive intelligence. Competitive intelligence shapes vision. Due to the speed of business in the modern organization, crisis is prevalent. Every crisis is a violation of vision, mission and values. Every crisis solution demands a modification, if not wholesale reworking, of strategy (vision, mission, values) and competitive intelligence activities. As the strategy and competitive intelligence disciplines come under more scrutiny, the need for a comprehensive crisis management system becomes paramount.

An effective, and well adhered to, business continuity management system provides value for the organization, by allowing it to adapt to the rapidly changing business environment we are faced with today. The speed of response to an event will determine the outcome, either positive or negative, for the organization. The ability to connect all of the elements in an organization during an event is essential for the success of the response. The value achieved through an organized management and response effort to an event is measured by the intangibles: perception, information, relationships, loyalty; it cannot be seen and often it cannot be measured.

Where's your next event crisis coming from? Learn about the key elements for developing an effective crisis management program for your organization.

Introduction

Companies are quickly learning it is important to have a Business Continuity Plan (BCP) in place to both prevent and respond to a variety of calamities that have the potential to create significant business interruption. The challenge for many companies is to determine what kind of Business Continuity Plan they should develop. Many companies will arrive at the answer to this critical question through a series of false starts, trail and error. Other companies often arrive at the answer by first defining what they mean by "*normal*" business operation, identifying the level of business interruption the company can sustain before its survival is threatened and identifying what "*recovery*" should look like for the company. Recovery can be defined as the ability to operate well enough to meet current obligations to one's clients at a level that is acceptable to clients, suppliers, vendors, business partners, your organization and to protect the life safety of your employees.

The ability to effectively respond to and manage the consequences of an event in a timely manner is essential to ensure your company's survivability in today's fast paced business environment. With the emergence of new threats, such as cyber-terrorism and bio-terrorism; and the increasing exposure of companies to traditional threats such as, fraud, systems failure, fire, explosions, spills, natural disasters, etc. an "*all hazards*" approach to Business Continuity Planning may be your best answer. The "*all hazards*" approach, as presented herein, is based on the concept of graceful degradation and agile restoration. By "*graceful degradation*" I am referring to the ability of your organization to identify the event, its consequences, establish minimal stable functionality, devolve to the most robust less functional configuration available in the least disruptive manner possible and to begin to direct initial efforts for rapid restoration of services in a timely fashion. The "*all hazards*" approach embraces consequence management as a key driving force.

Assumptions

Before we can discuss the elements of an "*all hazards*" Business Continuity Plan, some basic assumptions need to be presented. These basic assumptions, once established, will form the framework for the "all hazards" approach.

Assumption # 1: Businesses are complex systems operating within multiple networks
As depicted in figure 1, entitled, "Connections and Interdependencies", modern businesses are complex systems. These complex systems consist of five essential elements of analysis (EEA). The essential elements of analysis (EEA) are human resources, information resources, equipment and facilities. Each of these EEA can be further sub-divided into sub-units that provide measures of effectiveness (MOE) that can be further sub-divided to determine measures of performance (MOP). This subdivision can be continued to the level of raw data.

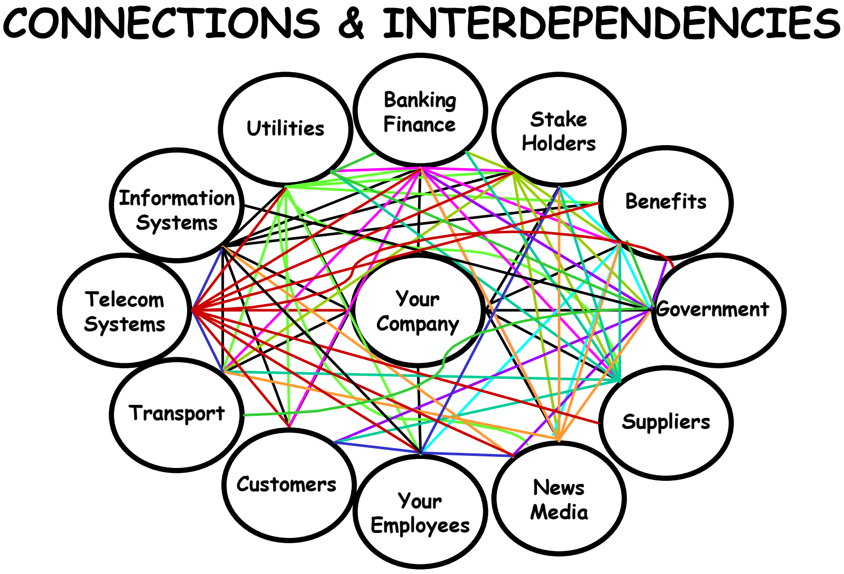
Assumption # 2: there are many layers of complexity
The complex business system can be viewed as being layered, wherein the outer layer is full functionality and the inner core is minimal stable functionality.

Assumption # 3: Due to complexity, analysis of event consequences is critical
All of a system's touch points within a given network must be considered in order to effectively evaluate vulnerabilities, threats, risks, hazards and determine the effects of degradation

Assumption # 4: actions need to be coordinated
Each company's actions within the network will be inadequate unless the entire network responds in kind.

Assumption # 5: Resources and skill sets are a key issues
Most companies lack the resources and specialized skills to know what to do to maximize positive network effects.

Figure 1: Connections and Interdependencies



The Facts

The following facts must be considered when developing an "*all hazards*" Business Continuity Plan.

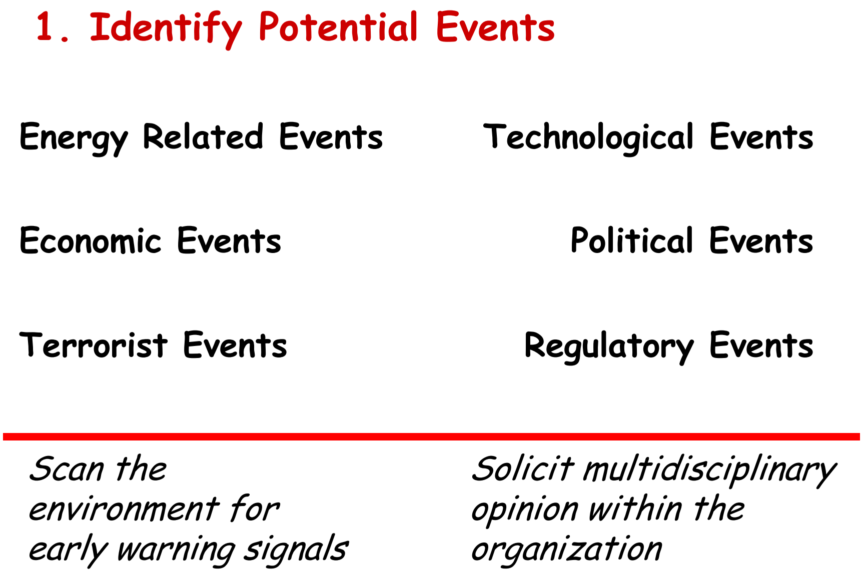
- Events that have been building since the end of World War II, including thousands of terrorist attacks on innocent civilians worldwide, have culminated (so far) in vicious and indiscriminate attacks first by domestic terrorists and now by foreign terrorists on the United States homeland.
- America is not immune from terrorism. Quite the contrary, we are a target rich environment for both domestic and international terrorists. The stakes are high, and the issues are indeed, life, death and economic survival.
- Terrorists are driven to kill people and to destroy property.
- All people and all facilities/operations, and therefore all companies are at risk.
- Priority terrorist targets are those of monetary or strategic value, having high human density and with cultural or symbolic value.
- Corporate headquarters of major corporations are prime targets.
- Corporations must take responsibility for their survival. Most of what has to be done in the corporate environment must be done by the corporation. Indeed, it is the corporation's responsibility to its people, stakeholders and to the public that relies on its products and services.
- Government, on the other hand, must concentrate its efforts on ensuring the protection and preservation of "critical infrastructures" essential to the nation's continued well being. These infrastructures are electric power supplies, gas and oil, telecommunications, banking and finance, transportation, water supply systems, emergency services and continuity of government.

- Corporate America must act now to make key assets (human resources, information resources, equipment and facilities) unattractive targets for terrorists. Failure to do so is be vulnerable to an attack.
- An "*all hazards*" approach to Business Continuity Planning will provide the most effective use of resources, can facilitate risk reduction and minimize the potential disruption to the complex network structure of modern business.

"All Hazards" Business Continuity Planning

The first step in preparing the "*all hazards*" Business Continuity Plan is to determine your organization's exposures. Simple as this may sound determining exposure is a complex process. In order to properly assess your organization's exposure you need to effectively evaluate vulnerabilities, threats, risks, hazards, and determine the effects of degradation to your organization. Figure 2, entitled, "Determining Exposure", provides an example of the initial actions that need to be taken in developing the "*all hazards*" Business Continuity Plan.

Figure 2: "Determining Exposure"



1. Identify Potential Events

Energy Related Events

Technological Events

Economic Events

Political Events

Terrorist Events

Regulatory Events

Scan the environment for early warning signals

Solicit multidisciplinary opinion within the organization

Ask yourself, in your opinion, what would be the ten most devastating surprises for your organization and its operations? In conducting this assessment a variety of scenarios need to be developed to assess the short term, intermediate term and long term effects of a disruption. This assessment should consider the following key factors as depicted in the Table 1, entitled, "LMS' CARVER Analysis Elements." The first element is "Criticality". A determination as to the criticality of the service, product, etc. being supplied via the value chain is essential, if you are going to adequately assess the potential risk exposure. Once criticality is established, an assessment of "Accessibility" is necessary. "Accessibility" refers to how easily one can get access to an Essential Element of Analysis (EEA).

One needs to assess the accessibility to the EEA, the accessibility to and of alternatives that can be substituted and the accessibility of the EEA to disruption. Once "Criticality" and "Accessibility" are established, you need to determine "Recognizability". That is, how readily recognizable is the

EEA with respect to its loss from your organization’s value chain. If I am targeting your organization, I am going to look at readily recognizable EEA’s that can be accessed and are critical to your operations. Once the first three items’ weighting parameters are established, one must determine the “Vulnerability” presented by the potential loss of the EEA in your value chain. For example let’s say you are a distributor and are concerned over critical inventory.

Your information systems may be able to accurately depict your inventory. However, if you were to lose access to your inventory supply location or ability to move the inventory to market it would not matter how accurately you could determine the level of inventory, as you and your customers would not be able to access the items. A “Vulnerability” can therefore be defined as the potential for any degradation, interruption or non-recoverability to such an extent that the consequence is likely to result in harm to the organization, harm to others (suppliers, customers, etc.) and/or substantial negative financial impact. A “Vulnerability”, therefore, can arise from a: false ASSUMPTION; blocked or altered COMPONENT; blocked or altered FUNCTION; or blocked or altered OPERATION.

Once you have established, “Criticality”, “Accessibility”, Recognizability and “Vulnerability” you must determine the “Effect” of the loss of the value chain item. “Effect” can and will generally be associated to the impact of the loss. However, one must consider all aspects of “Effect”, there can and may be some positive “Effect” that can arise from the loss or interdiction of the value chain. Lastly, one must determine the “Recouperability” aspects associated with the potential loss or disruption. How resilient is my organization? Can we quickly respond to, manage and recover from a disruption of the value chain? The net result of conducting a “CARVER Analysis” is to be able to determine the potential significance of an event from a consequence management perspective.

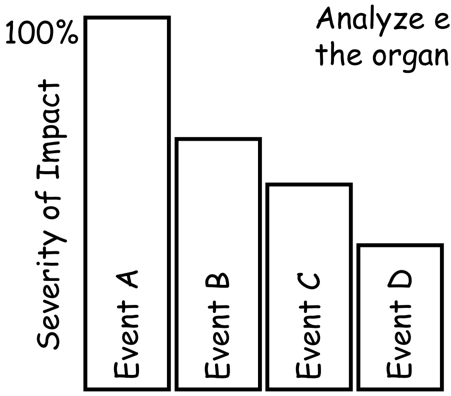
Table 1: LMS’ CARVER Analysis Elements

LMS’ CARVER Analysis Elements
C = Criticality
A = Accessibility
R = Recognizability
V = Vulnerability
E = Effect
R = Recouperability

Once exposures are determined and the CARVER Analysis is conducted, you should have a rank ordering of potential events, or a record of your worst nightmares if you care to think of them in that context. The next step is to put these “*nightmares*” into perspective. Figure 3, entitled, “Determine Potential Impact”, depicts the rank ordering of potential events and their worst case outcomes. In analyzing each event’s impact on your organization’s routine risks and touch points within the network your company operates in, you can begin to develop the focus for the “*all hazards*” Business Continuity Plan.

Figure 3: Determine Potential Impact

2. Determine Their Impact Potential



Analyze each event's impact on the organization's routine risks

Assume each event's probability of occurring is 100%

Upon conclusion of this step you should have developed decision making model similar to the one depicted in Table 2, entitled, "Decision Making Model".

Table 2: Decision Making Model

#	PROCESS STEP	END POINT RESULT
1	DEFINE THE DECISION	Describe what you need to decide
2	State Alternatives	Compile a list of decision alternatives
3	What are the Objectives	Compile list of desired objectives. State them in terms of what is preferred by you in the final outcome
4	Which Alternatives best meet the Objectives	Evaluate each objective. Rank alternatives, one relative to another, by your opinion as to how well each would meet a single objective. Create a ranking (A = best, B = second best, etc.)
5	Which Objectives are most important	Judge the value of the objectives using the same ranking system
6	Apply Relative Value	Combine judgment steps 4 & 5
7	Identify Best Choice	Add numbers across each row for alternatives
8	Make Decision	Review results; satisfy yourself that these are your best judgments

As you apply the Decision Making Model that you have developed, you should be able to develop a summary of potential events, probability of occurrence and potential impact on your organization. Table 3, entitled, "Disaster Exposure Rating Chart", depicts this product. The following chart summarizes the risks and/or threats to continuation of critical business functions considered relevant to the development of the "*all hazards*" Business Continuity Plan. The risks identified encompass the categories of **natural, technical** and **human** threats. For each risk, an estimate of the impact on critical business functions should be determined in terms of probability, impact (High, Medium, Low) and effect (Long or Short Term).

Table 3: "Disaster Exposure Rating Chart

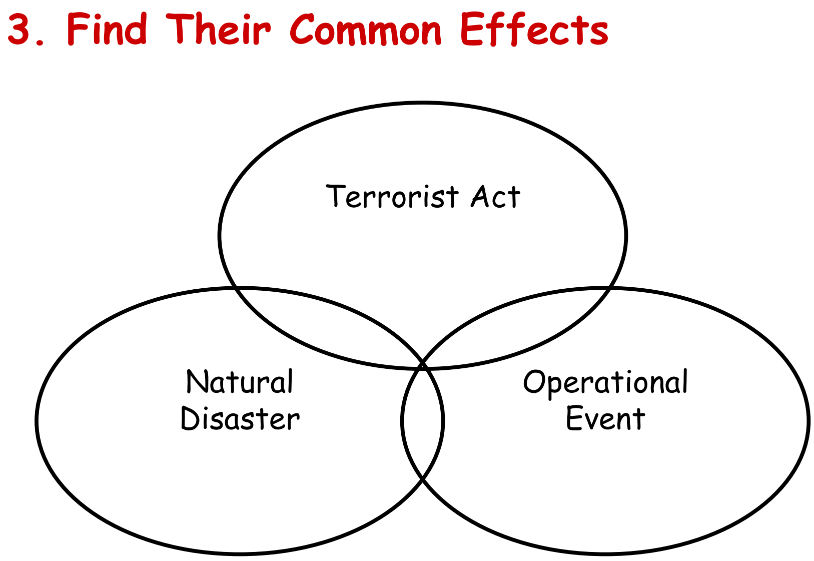
Risks/Threats	Probability	Impact	Effect
BOMB THREAT			
Customer Injury on Premises			
Data Entry Threat/Employee Error			
Disruption of Courier/Delivery Service			
Earthquake			
Explosion			
Fire			
Fraud/Embezzlement			
Heating/Cooling Failure			
Kidnapping/Extortion			
Lightning			
Loss of Critical Personnel			
Natural Gas Leak/Carbon Monoxide			
Power Failure			
Robbery/Assault			
Snow/Ice			
Software Failure/Virus			
Tampering with Sensitive Data			
Telecommunications Failure			
Terrorist Act			
Tornado/Wind Damage			
Unauthorized Access/Vandalism			
Water Damage/Rain Storms			
Weapons of Mass Destruction Event			
Workplace Violence			

The next step in the "*all hazards*" development process is to find the common effects that these events would trigger. As depicted in Figure 4, entitled, "Determining Common Effects", and by using LMS' CARVER Analysis tool, one can begin to determine effective strategies for event response, management, mitigation and recovery of business operations.

Once common effects are determined, developing response strategies can be accomplished. When determining response strategies consideration must be given to obtaining necessary information, determining priorities and values and preparing options for addressing the effects of an event. As depicted in Figure 5, entitled, "Develop Responses", this process entails the answering of six key questions. These questions are:

- **STRATEGY**: What are we committed to?
- **CONCEPT OF OPERATIONS**: How will we fulfill this strategy?
- **STRUCTURE**: Do we have the organizational structure that fits our needs?
- **RESOURCE MANAGEMENT**: How will we manage our resources (human, equipment, information, facilities)?
- **CORE COMPETENCIES**: What skills does our organization possess?
- **PRAGMANTIC LEADERSHIP**: How will we optimize authority, decision-making, workflow and information sharing?

Figure 4: Determining Common Effects



3. Find Their Common Effects

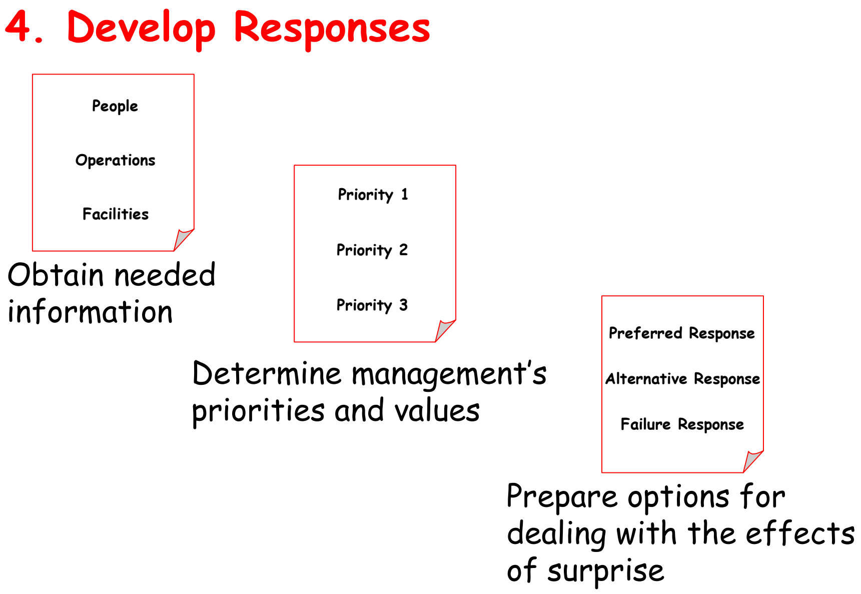
Terrorist Act

Natural Disaster

Operational Event

Answering these questions is not as easy as it seems. One must realize that in developing the "*all hazards*" Business Continuity Plan, certain commitments are going to be made. Fulfilling these commitments is critical to the success of the "*all hazards*" plan.

Figure 5: Determining Responses



4. Develop Responses

People

Operations

Facilities

Obtain needed information

Priority 1

Priority 2

Priority 3

Determine management's priorities and values

Preferred Response

Alternative Response

Failure Response

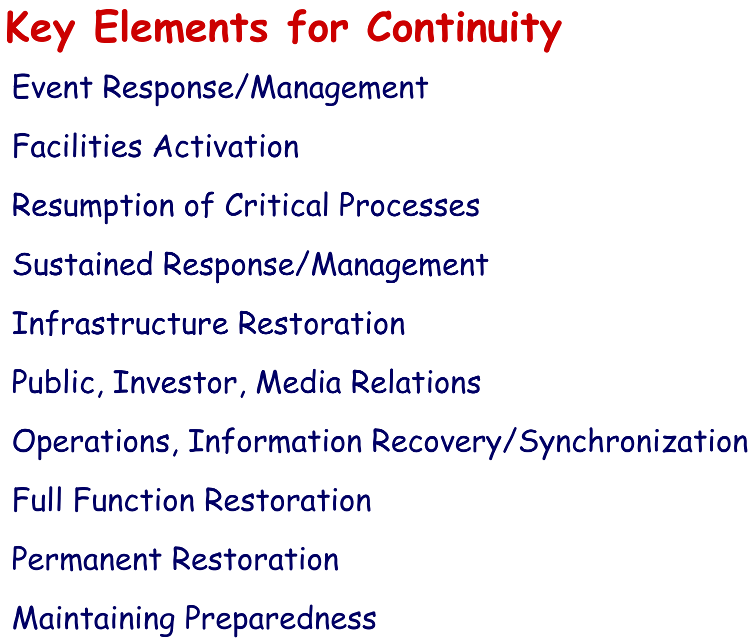
Prepare options for dealing with the effects of surprise

A key point to remember is that response reflects experience. Your organization will respond to events based on its experience in dealing with similar situations. It is therefore imperative that you consider the new threat environment that we are faced with today in determining the response options that you choose for the "*all hazards*" Business Continuity Plan.

"All Hazards" Planning Elements

Once you have accomplished the initial analysis and strategy determination phases, you are ready to begin to create the "*all hazards*" Business Continuity Plan documentation. Documentation of your efforts is critical to your success. You need to continually reinforce the concept of complex systems operating in a network as you develop the written elements of your plan. While there is no prescription for the contents of the plan, I have found that the following elements seem to be common to all plans in varying degrees of detail. These common elements are depicted in Figure 6, entitled, "Common Planning Elements". A brief discussion of each of these elements follows.

Figure 6: Common Planning Elements



Key Elements for Continuity

Event Response/Management

Facilities Activation

Resumption of Critical Processes

Sustained Response/Management

Infrastructure Restoration

Public, Investor, Media Relations

Operations, Information Recovery/Synchronization

Full Function Restoration

Permanent Restoration

Maintaining Preparedness

- **Event Response/Management**: Critical to the success of the "*all hazards*" BCP is the ability to respond and manage an event. Initial response to an event is a critical success factor. How your organization responds and communicates this response throughout the organization and its network is one of the determining factors in how well you will manage subsequent phases of the disruption. This portion of the "*all hazards*" BCP should be designed to provide guidance for key personnel to prepare initiatives for early response to an event affecting the organization and its assets. The primary mission of event response is to assess, evaluate, contain the event and seek to control the outcomes of the event. Total management support through all stages of the event response/management process in order to minimize the adverse impacts of a business interruption to the organization is a critical success factor. As such, a seamless vertical and horizontal communication system based on common terminology and streamlined communication contact needs to be developed to underwrite the BCP. In order to facilitate communication common terminology should be developed for such things as how the organization defines an event, classifies its severity and determines response options. Remember that these definitions need to go beyond the organization and include the network that the organization operates in.

- **Facilities Activation**: Once activated where does the organization conduct its operations? Your plan needs to address the activation of facilities for the overall management of the event, the provision of technical support, business systems relocation, rumor control, and media management to name but a few.
- **Resumption of Critical Business Processes**: Based on the use of LMS' CARVER Analysis and assessments that you have conducted, you will have established a list of critical business functions. You need to determine how you will re-establish your critical business processes. Table 4, entitled, "Phases of Response", depicts common activities to consider when identifying and determining the critical business processes that need to be resumed.

Table 4: Phases of Response

Phases of Response	**Activities**
Initial Response	Incident Notification & Incident Response Activation of CMT. Declare "Crisis" by level of severity
Sustained Response	Command Center Activation. Business Impact Analysis. Recovery Planning.
Recovery Phase 1	Assessment of Actual Damages/Impacts. Identification of Critical Processes and Critical Infrastructures
Recovery Phase 2	Restoration of Critical Processes. Infrastructure Restoration. Info/Ops Recovery/Synchronization
Deactivation/Termination	Full Function Restoration. Permanent Restoration Deactivate & Terminate "Crisis" level of severity

The timeframe of each phase may vary widely, dependent on the event and the resources available to respond to the event. For the purposes of discussion the following timeframes are used as a baseline. The timeframes depicted in Table 5, entitled, "Response Timeframes", are used as guidelines only. Each event should be addressed separately, according to the impact and assessed effects as determined by your organization.

Table 5: Response Timeframes

Response Timeframes	**Estimated Duration**
Event	One (1) Day
Command Center Activation	One (1) Day
Initial Response	Three (3) Days
Restoration of Critical Processes	Twenty (20) Days
Infrastructure Restoration	Thirty (30) Days
Info/Ops Recovery/Synch.	Twenty (20) Days
Full Function Restoration	Forty Five (45) Days
Permanent Restoration	Ninety (90) Days

Assuming an event lasting approximately one day with an event response lasting approximately three days, an organization should be able to begin Command Center activation (assuming availability of Command Center location) on or about day one. With the additional activation of "Hot Sites" for information technology functions and facility relocation operations, this process is estimated to last approximately five days before the all sites are fully activated and operational. At day five of the "Crisis" the restoration of critical processes is begun. This assumes that critical processes are identified and access to the affected area to accomplish surveys and determine the level of degradation of critical processes. Critical Processes should be operational by day twenty-five of the "Crisis". Commencing parallel to the restoration of critical processes is Information/Operations Recovery and Synchronization. The recovery of information/operations and subsequent synchronization assumes that loss data can be identified, backups are accessible, and access to the affected area is available to determine the amount of loss. Information/Operations Recovery and Synchronization should be accomplished by day twenty-five of the "Crisis". Infrastructure Restoration should be accomplished by day forty-three of the "Crisis", assuming access and availability to required non-Company resources. By day forty-five of the "Crisis", Full Function Restoration can be completed, assuming that Restoration of Critical Processes, Infrastructure Restoration, Information/Operations Recovery/Synchronization have been accomplished or are well underway. Permanent Restoration may take up to ninety days or longer. If the Permanent Restoration process is started by day seven of the "Crisis", it should be accomplished by day ninety-seven.

- **Sustained Response/Management**: Critical to your ability to successfully execute your "all hazards" BCP will be sustaining response and management efforts. In order to sustain response and management functions your organization must take control of the event. Until you are able to take control of the event, your organization will be in a constant state of reaction. Figure 7, entitled, "Elements of Response", depicts some of the key aspects that must be achieved in order to sustain response and management functions.

Figure 7: Elements of Response

Pre-Incident	Reactive	Proactive
Preparation	**Initial Response**	**Sustained Response**
Analysis	Chaos Control	Sustain & Augment
Planning	Identification	Specialize Teams
Resource Identification	Defensive Actions	Offensive Actions
Training	First Response	Forward Planning
		Resource Management

It should be noted that in today's business environment we are seeing a change in the response paradigm. As business change accelerates, it is getting more and more difficult for traditional strategists to achieve an accurate focus on the current situation. Strategy in the traditional sense is outdated before it can be implemented. Speed, operating at real-time, is pushing traditional strategy development, forecasting, competitive-intelligence collection, and analysis to new limits.

Vision, mission, and values are important for every organization. They shape strategy for the organization. Strategy, in turn, is influenced by information in the form of competitive intelligence. Competitive intelligence shapes vision. Due to the speed of business in the modern organization, crisis is prevalent. Every crisis is a violation of vision, mission, and values. Every crisis solution demands a modification, if not wholesale reworking, of strategy (vision, mission, values) and competitive-intelligence activities. As the strategy and competitive-intelligence disciplines come under more scrutiny, the need for a comprehensive business-continuity management system becomes paramount.

The ability to sustain the response to and management of an event provides value for the organization, by allowing it to adapt to rapidly changing situations. The speed of response to an event will determine the outcome, either positive or negative, for the organization. The ability to connect all the elements in an organization during an event is essential for the success of the response. The value achieved through an organized management and response effort to an event is measured by several intangibles: brand image, perception, information, relationships, and loyalty to cite a few. These intangibles cannot be seen, and often, they cannot be measured.

♦ **Infrastructure Restoration**: Internal and external infrastructure is important to an organization's success during normal operations. Infrastructure is essential to an organization's success during an event. The problem that most organizations face is relatively simple. Your organization does not control, to a great extent, the infrastructures that contribute to the success or failure of event response. Cited earlier were critical infrastructures that have been designated by the Federal government as essential to maintaining national security. These very same infrastructures are essential to your organization's business survival. To briefly recap, they are electric power supplies, gas and oil, telecommunications, banking and finance, transportation, water supply systems, emergency services and continuity of government.

In order to assure infrastructure restoration in a timely manner, an organization needs to determine the capability of its network to address the restoration of the above identified critical infrastructures and to assess and determine the effort required to restore its internal infrastructure. Without infrastructure an organization is on a path to failure.

♦ **Public, Investor, Media Relations**: Stakeholders are those that have a vested interest in your organization's success in responding to and managing an event. If this element is not addressed as a part of your current business continuity planning effort, make it a priority to address. The "*all hazards*" concept includes the "*crisis media*" element as an integral part of the overall plan. An inadequate response to the external stakeholders by your organization can negate an effective response.

The phrase "*Perception is reality*", is never more true that when your organization is under public scrutiny. In order to address this planning element, it has to be addressed early on in the planning process. The following list is an example of stakeholders that need to be considered as you develop your organization's "*all hazard*" BCP.

♦ **Operations, Information Recovery/Synchronization**: Because of the tremendous importance placed on information management in today's business environment a great deal of emphasis is placed on recovery and synchronization of information systems. Similarly, the same amount of emphasis should be placed on getting operations recovered and running. Most businesses do not do this. It is assumed that the operational portion of the organization will recover.

In today's threat environment this is not the case. It is imperative that the organization seeks to recover and synchronize its operations and information systems. This can be a very daunting task for many organizations. Consider the implications of inventory, transportation, facilities, equipment and you begin to see the need to address operations as strongly as you address recovery and synchronization of information systems.

- **Full Function Restoration**: The resumption of business operations following the mitigation of an event requires a transition from response/management to re-entry and recovery. The recovery organization requires different skills and has a different perspective that the response and management organization. Effective recovery planning should be part of your initial planning effort. One of the main goals of your "*all hazards*" BCP should be making effective preparedness activities a way of doing business not an adjunct to the business and/or to a business disruption.

  You must address recovery operations in your business planning documents. It is too late to start after the incident has occurred. "How can I know what to plan for?" might be a question that comes to mind as you read this paragraph. Well, if you have performed an effective hazard, vulnerability and risk analysis you should be able to say, "I've got the basis for my recovery planning here in front of me."

  What Constitutes a Good Recovery Plan? Herein lies a quandary. A good recovery plan for what? A corporate office complex? A community? A plant site? The list can go on and on. Perhaps we should consider the following definition for recovery planning/post-incident operations before we bound off on the key elements of effective recovery planning.

  > **Recovery/Post-Event Operations:** *All operations designed to support the termination, reentry, recovery and humanitarian assistance requirements arising from an event. This may include, but is not limited to: establishing a Recovery Organization, addressing the transition of the response and management organization into an organization focused on reestablishing the primary/normal function of the organization.*

  Recovery or Post-Event Operations begin when the event has been brought under control. Notice I did not say "mitigated" or "terminated". "Control" is the operative word. Once you have gotten ahead of the event, you can begin to start refocusing your resources and channeling them to post-event related issues. The key elements for effective recovery planning are Effective Hazard Analyses, Recovery Organization, Recovery Pre-Plans, Strategic Focus, Human Factors Considerations and Superior Communications Capabilities.

  Once full function is restored your organization can begin to think about getting back to business as usual.

- **Permanent Restoration**: Permanent restoration is accomplished when the organization determines that it is operating at the same level or acceptable levels to declare the event terminated. Generally, the business operations and information systems are synchronized and the organization is capable of normal (pre-event) business activities. During the permanent restoration phase, an assessment should be made to determine performance parameters and to re-evaluate vulnerabilities, threats, risks and hazards. The assessment should also evaluate business network considerations.

- **Maintaining Preparedness**: The process of business continuity planning is unending. Once developed, the BCP must be constantly evaluated, updated and maintained current. Part of this process is the development of the human resource component of the organization. A trained and educated workforce can do more to protect your enterprise than you can imagine. Training of personnel is a critical component of the "*all hazards*" approach to business continuity planning. Training and educating your personnel at all levels is one of the critical success factors that must be addressed if an adequate response to an event is to be achieved. A "*Systems*" approach to preparing effective training programs should consist of:

- ***Task analysis****:* When designing an integrated training program, first determine the skills, knowledge, and procedures required for satisfactory performance of each task.
- ***Lesson Development****:* Learning objectives are defined from the skills, knowledge, and procedures developed during task analysis. Instructional plans are then prepared to support the learning objectives.
- ***Instruction****:* Lessons are systematically presented using appropriate instructional methods. Instruction may include lecture, self-paced or group-paced mediated instruction, simulation and team training.
- ***Evaluation****:* Performance standards and evaluation criteria are developed from the learning objectives. Each trainee's performance is evaluated during the course and during field-performance testing.

In addition to formal training programs, a program of proficiency demonstration to validate the training and content of plans is also needed. This can be accomplished by establishing a program that supplements the training with simulations (drills and exercises).

Consider developing programs to educate your employees on basic life safety (first aid, CPR, Evacuation, Assembly, Accountability), what to do if an event occurs and what to do after the event. In addition, a community outreach program can provide your organization with many benefits.

A community outreach program can enhance coordination with local emergency response and law enforcement agencies, put your organization in a positive light in the community and provide your employees more information on community resources.

You cannot stop at classroom training and expect your organization to respond effectively to an event. Corporate America needs to assess how prepared it is to deal with workplace events. The government must focus its attention on the protection of critical infrastructures and international issues.

Corporate America has to address protective measures that ensure its survival; it cannot depend blindly on the government to be there for assistance. Being able to respond appropriately will be essential, however, responding without the proper equipment can lead to failure. You need to equip your workforce with the appropriate emergency response equipment, such as first aid kits, fire extinguishers, event response kits, and evacuation, assembly, accountability procedures.

You should also understand that when you purchase the equipment and train your personnel on its use, you have to develop and implement a maintenance program to assure that the equipment is there and that it works when it is needed.

Critical Functions in the "All Hazards" BCP

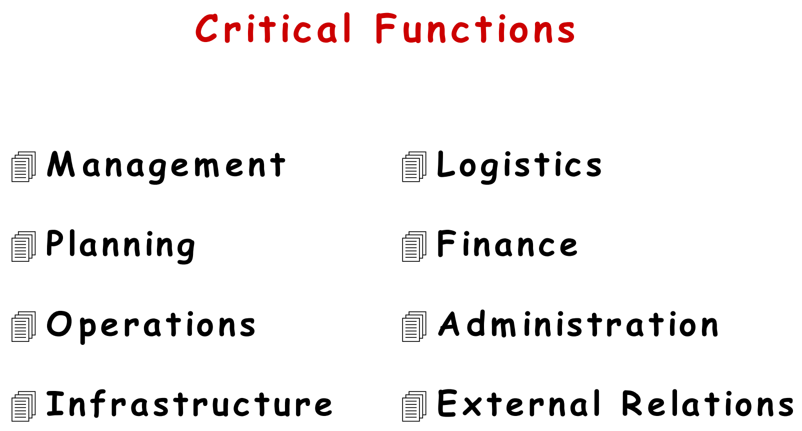
The ability to implement the "*all hazards*" BCP concept is based on a flexible plan and a focus on critical functions to be performed, not on organizational line an block type charts. An organization must address the development of a response/management and recovery organization based on performing critical functions during and after an event. This may be the most difficult task for an organization to accomplish, especially with reorganization and down-sizing to contend with.

The critical functions that an organization must address can be categorized into eight areas. Figure 8, entitled, Critical Functions", illustrates these. A brief discussion of each function that must be address is provided herein.

♦ **Management**: Someone has to be in-charge. However, the organization needs to determine who and at what level and in-charge of what. This leads us back to our six key questions. Recall the last question, regarding the optimization of authority, decision-making and information sharing? The Management function has to address this issue. Without effective decision-making, optimization of authority and information sharing chaos has an excellent chance of prevailing.

Some of the key Management functions that need to be addressed are optimization of authority, decision-making, communication, assessment of event conditions and classification of the event as to severity. Other Management functions should focus on determining legal requirements and identifying issues that need to be resolved. Management is never put more strongly to the test than in a crisis situation. The objectives are immediate and the results have long term implications. Today, individuals responsible for the management of businesses and public agencies must be prepared to deal effectively with threats that could not be conceived of prior to September 11, 2001.

Figure 8: Critical Functions



Critical Functions

- Management
- Planning
- Operations
- Infrastructure
- Logistics
- Finance
- Administration
- External Relations

Once the Management function is defined, the next area to address is the Planning function. The Planning function embraces, long-term strategic planning, as well as, short-term tactical planning. Incorporated in the Planning function should be an analysis of competitive intelligence with regards to the information that your organization may potentially give up as a result of how it responds to and manages the event. Most of the value-added in business today is created by knowledge-based service activities, such as research and development, marketing research and customer information to cite a few. The development and implementation of a Strategic Plan charts the course your organization will use to move into the future. Mission, vision and values are reflective of Strategy. Competitive Intelligence, the acquisition and/or denial of information, is an integral part of the Strategy process.

Business Continuity Planning (crisis management in a broad sense) is the ability to deal effectively with events that threaten the operation of business, is an integral part of the Planning function.

Vision is important to organizational success. Competitive Intelligence shapes vision. Crisis is prevalent in modern organizations. Every crisis your organization experiences is a violation of Strategic Vision. Every crisis therefore demands a modification of Strategy and Competitive Intelligence Initiatives.

- **Operations**: Once the Management function and the Planning function are addressed, the Operations function must be considered. The Operations function is relatively straightforward. This function must take in to account affected operations and unaffected operations. The focus should be on event mitigation, support of response operations, preventing the event from cascading and continual evaluation of options.

- **Infrastructure**: With today's dependence on internal and external infrastructures, it is important to designate this a critical function with the BCP. The Infrastructure function should consider all available internal and external infrastructure requirements. A close liaison with external infrastructure providers should also be addressed by this function.

- **Logistics**: The old saying is, "An army lives on its stomach", or some words to that effect. This is true with your organization and its ability to respond to an event. The Logistics function should address the short-term needs of the organization and any long-term needs that the organization requires. These include, but are not limited to, equipment needs, facilities requirements, human resource needs, housing (temporary and long-term), and communications needs.

- **Finance**: Establishing a cost tracking system to determine how much is being spent and where it is being spent is important to the long-term survival of the organization. During an event unchecked costs can cripple an organization. Delays in getting financial resources to involved entities can cause the response, management and recovery efforts to grind to a halt. The Finance function should be focused on establishing a streamlined finance and accounting system that can track expenses and expedite payments.

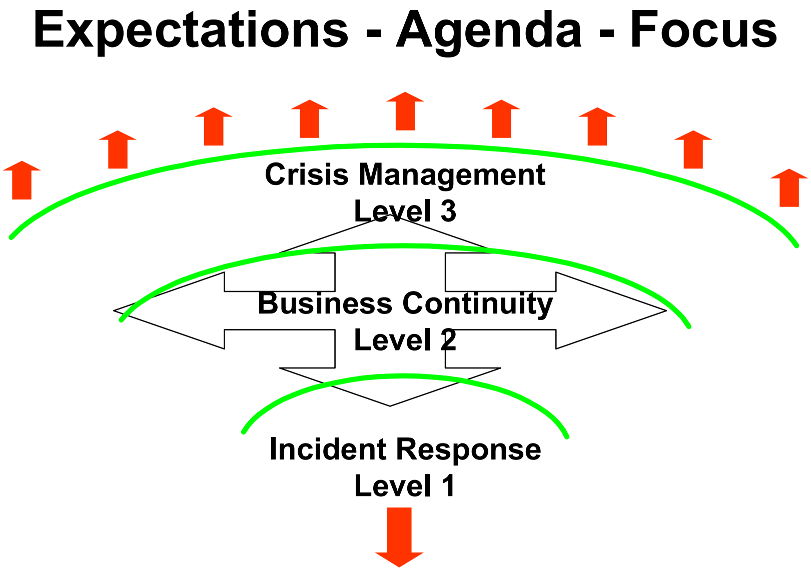
- **Administration**: The Administration function should focus on resource management, documentation and other administrative aspects. Often overlooked as a critical element, the Administration function provides tremendous support to the success of response, management and recovery efforts. And, as someone once confided to me, "they know how everything works!"

- **External Relations**: The External Relations function serves as a liaison to all entities with a vested interest in the organization's response, management and recovery from the event. Often restricted to media relations, this function should be expanded to perform liaison and information sharing with all stakeholder entitles.

Figure 9, entitled, "Expectations, Agenda and Focus", provides an example of the various levels within an organization where the above-cited critical functions need to be tiered and replicated. At the event response level, the critical functions are primarily focused on event containment and mitigation. The expectations at this level are for assistance from the next level in the form of resources and support. The agenda and focus at this level is relatively simple – contain and mitigate the event. At the next tier or level, the expectations, agenda and focus change. The critical functions need to begin to manage upward and to address horizontal issues, such as the prevention of the cascading of the event. The expectation is to get sufficient information communicated from the event scene to enable decision-making that enables the unaffected portions of the business to continue to operate unencumbered. The agenda and focus have expanded to include longer term assessment, unaffected operations and expanded communications. At the top level, the expectations, agenda and focus are completely different than at the event level. At this level the expectations are for information that can be useful in addressing stakeholder concerns. The agenda and focus are almost totally directed outwards toward external audiences. It is critical that effective communications is part of the "*all hazards*" BCP. Seamless vertical and horizontal communications does not mean, just the ability to connect. It means that a common terminology is employed to ensure that the communications are understood by all who receive them.

As depicted in Figure 9, there are a series of waves that overlay the three levels. These waves represent the cumulative effect of an event as it ripples through an organization. It should be noted that the further away from the event the greater the effect of the wave. What this means is that the higher an event gets within an organization the greater the repercussions and effects that are felt. Again, an effective communication system based on common terminology, coupled with an effective event classification mechanism can serve to facilitate more effective response, management and recovery operations.

Figure 9: Expectations, Agenda, Focus



Concluding Remarks

In almost every instance of successful response to an event, response, management and recovery activities consisting of sound operating execution coupled with superior communication predominate.

Operational response is essential. It is the one that saves lives, property and other assets. The ability to communicate is no less important. It is the one that saves the business.

The simple fact is *perception is reality*. Public perception of your company's reaction to an event is as important as your operating response. Lessons learned from a wide range of events occurring over the past thirty years validate the need for a dynamic business continuity plan.

An effective BCP consists not only of the plan documentation, but also of the human, equipment, facilities, operations and information elements; and the critical functions that must be addressed. An effective BCP is one that: provides a shared, organized system of management; is a template for doing things right; is a comprehensive process with a common and easily understood terminology; provides effective coordination of activities among entities, early warning and clear instructions for action; and provides continued consequence assessment.

References:

"September 11 Aftermath: Seven Things Your Organization Can Do Now", published in Disaster Recovery Journal, Winter 2002, Volume 15, Number 1

"September 11 Aftermath: Ten Things Your Organization Can Do Now", John Liner Review, Winter 2002, Volume 15, Number 4.

Davis, Stanley M., and Christopher Meyer, *Blur: The Speed of Change in the Connected Economy* (Boston: Addison-Wesley, 1998).

"It Can't Happen Here: All Hazards Crisis Management Planning", Geary W. Sikich, PennWell Publishing 1993.

"The Emergency Management Planning Handbook", Geary Sikich, McGraw Hill, 1995.

Critical Infrastructure Vulnerability - An Overview of the Findings of the President's Committee on Critical Infrastructure Protection, Geary Sikich, Independent Liquid Terminals Association '98, 1998.

Business Continuity & Crisis Management in the Internet/E-Business Era, Geary Sikich, Teltech, 2000

Author Biography

Geary W. Sikich gsikich@aol.com is the author of ***It Can't Happen Here: All Hazards Crisis Management Planning*** (Tulsa, Oklahoma: PennWell Books, 1993) and the ***Emergency Management Planning Handbook*** (New York: McGraw-Hill, 1995), available in English and Spanish-language versions. Mr. Sikich is the founder and a Principal with Logical Management Systems, Corp., based in Munster, IN. He has over 20 years experience in management consulting in a variety of fields. Sikich consults on a regular basis with companies worldwide on business continuity and crisis management issues. He has a Bachelor of Science degree in criminology from Indiana State University and Master of Education in counseling and guidance from the University of Texas, El Paso. Since its inception in 1985, Logical Management Systems, Corp. believes that a strategic approach to event management, involving careful analysis can help to avoid problems and transform issues into opportunities. We have helped many organizations develop and implement effective event management programs. www.logicalmanagement.com