

Crisis Management and the Emergency Operations Plan

by

Don H. Donaldson, RPA, CIC, CRM, CHS-III
(Originally published in *ROUGH NOTES*, December 2004)

Crisis response is a risk reduction technique within the broader context of risk control. Like any risk reduction technique, there is a presumption that there will be some type of loss producing event, i.e., a crisis, and the focus is to minimize the human and financial impact once the event takes place. The stakes are high and realities are harsh for companies that fail to actively plan for catastrophic events. Studies have confirmed that if a business cannot maintain continuity of core operations or must cease operations and/or close down for more than one week as a result of a disaster, over 40 % of those entities never reopen. Additionally, almost 30% of businesses that fall within this unfortunate group that succeed in reopening for business, will close for good within 2 years of the shut down.

Experienced risk managers have learned that there are two outcome critical components required to effectively respond to and recover from a crisis or disaster situation. The first is effective pre-event or pre-crisis planning that culminates in an written Emergency Operations Plan (EOP) that is disseminated to *all* employees and *every* entity that is required to ensure the recovery and viability of the organization. The second is pre-loss testing by the use of practice drills and mock implementation of the EOP. The mutual dependence and importance of both of these components cannot be overstated, however, this article focuses on the considerations in developing or updating an EOP.

Planning Framework

In order to provide some framework for the pre-event planning process, it is useful to think in terms of a triangle consisting of: Purpose -Scope -Goals. Pre-event planning, especially for organizations without an existing EOP, can be a daunting task. Focusing the process in this manner provides a workable framework:

- Purpose. What is purpose of the EOP? Does management require the EOP to play a mission critical role in the company s' survival after a disaster or is the plan expected to mitigate employee s' exposure to physical hazards only? The commitment of an organization s' resources to accomplish the former will necessarily be greater than to accomplish the latter.
- Scope. Will the EOP be a limited plan designed to address natural and/or environmental disasters? Will the plan encompass technological, political, or public relations crisis? The tendency of many risk managers, human resource mangers and other first time participants in the process of developing an EOP is to narrowly define the purpose of the EOP. Our experience, however, has indicated that most organizations achieve better overall results by expanding the scope of the EOP to address as many disaster scenarios as possible.
- Goals. What are the minimum and maximum parameters that will be used to measure the success or failure of the EOP? Minimums requirements are the outcomes that are *expected* with every implementation of the EOP. In this context, maximums are the

best case scenarios that can be expected for a particular crisis or disaster. It is important to consider the goals at both ends of the spectrum to ensure that the EOP is sufficient in scope and appropriate in purpose. If a goal cannot be consistently achieved in pre-event testing or practice drills, additional resources (time and/or money) must be applied to the post-event response/treatment or the goal(s) should be revised.

The EOP should represent the company's best attempt to implement the corporate priorities as stated by the company's top executives. Obviously, during this initial phase, senior management will be responsible for establishing or interpreting the corporation's goals and objectives that will become the framework for all other aspects of the EOP. A successful EOP will depend on a high level of commitment by the company's senior executives throughout the process.

Categorize Potential Emergencies

Once the initial framework for planning has been determined by company management, the next step is to begin the process of threat identification to be addressed by the EOP. Again, this process can seem initially overwhelming but most experienced risk managers agree there are some logical classifications to threat grouping that can be used in this phase of EOP development. This classification scheme allows for emergencies or threats of a common nature to be grouped together for identification purposes and, very often, be treated together from the standpoint of risk control techniques. The five general categories are:

- I. Historical. What has occurred in the *community* and/or region in the past. *Community* should be read to mean similarly situated businesses or entities. In this context, it may be important to consider the experience of peer companies and competitors that are not necessarily in the same geographical region or proximity.
- II. Geographical. The obvious considerations would include exposure to seismic events, coastal/flood waters, or atmospheric extremes (snow, ice, tornado, wind, etc.). Within this category, consideration should include any unique factors relating to the physical location of the key facilities or the source(s) of the employee population. If a significant number of the mission critical employee population must cross a bridge or utilize a singular/unique transportation method to reach the entity's operations facility, a successful EOP must anticipate the failure of such systems and incorporate appropriate response measures.
- III. Technological. Computerization during the past twenty years has elevated the importance of this category for all governmental and private entities, however, the old fashion low tech emergencies should not be overlooked. Basic services like electricity, fresh water, waste disposal, and old fashion telephone lines still form the backbone of modern business survival.
- IV. Human Error. Arguably, all failures in crisis or disaster response result from human error, however, for the purposes of categorization, it is useful to think in terms of how the entity would be impacted by such obvious things as: failing to lock the building, an employee's noncompliance with local, state or federal laws, libel/slander. Equally important are the not-so-obvious human errors like: physical harm done to or by an employee or to anyone within the operational facilities, civil or criminal negligence by an employee that could

result in vicarious liability to the entity, allegations of inappropriate or scandalous conduct by a senior executive –even if such alleged conduct may not directly relate to the employment of the person or persons in question. The impact to a company as a result of the chief executive officer or a member of the board of directors accused or charged with sexual indecency with a minor, or involvement in a hit and run auto pedestrian case can be as great as any natural disaster.

- V. Physical. What types of emergencies might result from the design or features of a particular facility? Are operations conducted in proximity to identifiable hazards or exposures that are not within the control of the entity in question? If a catastrophic situation developed would the concentration of mission critical employees at a particular location or facility be a factor in both the potential recovery and perhaps even the survival of the organization in question? Before 9/11, there was very little thought given to the particular problems associated with the density of employee populations, however, based on the tragic lessons of 9/11, many large companies have started to incorporate this type of consideration into their pre-event planning.

Identifying Critical Products, Operations, and Services

Once the corporate policy has been established and the threats have been classified by logical categories, the EOP must address the mission critical components that will be required for a successful post-event recovery. Many of these components will be fairly obvious, i.e., basic utilities, facilities for temporary/emergency operations and necessary equipment and personnel to implement the EOP and recovery plan. Depending on the type of organization, it may be important to incorporate supply and/or distribution chain components and vendors into the EOP for two reasons. The first is that your organization's survival may be dependent on one or more outside vendors as part of its ongoing operations, and therefore, its post-event recovery. The second, and frequently overlooked reason, is that a crisis or disaster that befalls one of your core suppliers or vendors may affect your organization even if your company does not directly suffer the same crisis or disaster. A fire or natural disaster across town or across the globe that shuts down a mission critical supplier can cause more financial harm than if the crisis occurred locally.

Other Considerations and Potential Resources

There are, or may be, other resources, references, and documents within your organization that may be impacted by the EOP or may be of assistance in developing the EOP. At a minimum, it is a good idea to obtain and review the following types of materials:

1. Employee manuals
2. Security procedures
3. Fire protection systems/manuals
4. Risk management plan
5. Insurance policies or programs
6. Hazardous materials handling

7. Purchasing procedures
8. Financing agreements
9. Hold harmless agreements
10. Leases/rental agreements
11. Service contracts and/or maintenance agreements
12. Accounts for all utilities – be sure to consider utilities that may be provided by the landlord or as part of a commercial lease.

Avoiding Common Mistakes

Studies of the unsuccessful outcomes of organizations that had an EOP in place prior to a crisis or disaster indicate there are three common factors associated with post-event failures:

1. Lack of Upper Management support/participation in recovery effort;
2. Emergency Response Teams (ERT s) did not have specific assigned tasks or did not have the resources to accomplish their specific tasks; and
3. Failure to update, revise and disseminate the EOP to ALL employees & mission critical clients/customers/vendors/suppliers. (Don t’ forget financial partners, affiliates, and subsidiaries).

Even well financed and responsibly run companies will not survive a major crisis or disaster without an effective EOP. Using the techniques discussed in this article, any company can successfully work through the process of creating an EOP that will be the cornerstone of corporate survival and recovery should the worst befall the organization.