

The Four P's of Crisis Preparation

September 2006

By Gerald Baron

Founder & President of AudienceCentral, inventor of PIER

Maybe it's because I was a teacher eons ago, or perhaps it's just that I am simple-minded, but I find it considerably easier to remember things when they all start with the same letter. For example, in my new book Now Is Too Late 2, I refer to the three main forces that cause today's crisis communicators the most trouble as the three I's: Instant News, Infotainment and the Internet. Therein, I outline the four elements of crisis preparedness as the four P's: Policy, People, Plan and Platform.

POLICY

Companies and organizations must think through in advance of any crisis the objectives they wish to achieve. A policy statement should incorporate the goals and/or aspirations of the organization going through a crisis and include the basic strategies they will employ to achieve these goals. The best policies are those that articulate the goal of emerging from a major crisis not only with the organization's reputation protected, but enhanced. Therefore organizations must meet these objectives by responding effectively as well as by communicating quickly, transparently and frequently with all critical audiences. Policy statements need not be long and fancy. In fact one of the best was expressed by a Head of Public Affairs for a Coast Guard district when he said, "We want to be the first and best source of maritime news," in reference to the event they were involved in. A swift and concise policy leads to the excellent reputation enjoyed by the Coast Guard for professionalism and responsiveness.

Policy statements can also include basic do's and don'ts of crisis communication. Here are a few examples:

- We will never release the names of employees involved in injuries or loss of life.
- Only authorized spokespersons that have been properly trained will be allowed to speak on behalf of the organization.
- We will always do our utmost to provide the most complete, accurate and timely information about the company and the incident.
- We will never abandon our commitment to honesty and the maintenance of trust our stakeholders have placed in us.

A few simple policies all with the unifying goal of building credibility and trust serve as memorable guidelines for all employees as well as outside consultants contracted during a crisis situation.

PEOPLE

Time and again the debrief after a crisis incident points to the people involved in responding and communicating as a key element. Whether your company or organization comes through a crisis with its reputation intact or enhanced depends largely on the leadership, skills, common sense, and character of the people involved in managing the response. This is why one of the most prudent things CEO's can do to prepare is to identify a crisis response team and prepare them for the roles they will play. These people will frequently have to act fast and with considerable autonomy. They will also have to play well with others. CEO's must look long and hard at these people. Will they make the right decisions? Will they take the initiative to do what is needed when it is needed? Will they behave in ways that will lead outside audiences and key stakeholders to trust the organization and its leaders? If a CEO does not feel comfortable with the answers to those questions, there is nothing more practical he or she can do than to make the needed changes before the critical crisis occurs.

PLAN

Most preparation focuses on the plan, and the plan is indeed very important. However most crisis plans are far too complicated. They sit in big red binders on the shelf and may or may not be pulled down and referred to during an event. If you cannot access your role within a single page of the plan—it's probably too complicated. If you cannot quickly get at the key information needed, such as who to contact and how to contact them, then it is of limited use. And furthermore, if it isn't with you or accessible when you most need it, the plan is useless.

A good crisis plan is structured like the inverted pyramid you may have learned in journalism school. It starts with a few basic elements that cover everything that ought to be included and subsequently executed. It then proceeds to deeper levels of detail until all applicable situations are covered. I also favor a cookbook style which includes the listing of action items that must be taken and who is responsible for carrying them out. Most plans I have written anticipate three levels of crisis, but all are based on the same simple plan that is very scalable.

To make the crisis plan accessible, put it on the internet. Of course it must be in highly secured forms such as on a secure company intranet, or better yet on a crisis communication control center as described in the next section.

I strongly believe that crisis communication plans should take advantage of the best thinking on this subject. Personally, this leads to the Incident Command System. This basic and very scalable management structure was developed out of the multi-agency response to forest fires in the 1970's, but since has been adopted by most fire, police, and government agencies. In fact, in 2003 the Department of Homeland Security mandated its use for all government agencies receiving federal funding. Therefore, if you are not familiar with the National Incident Management System (NIMS) and the Incident Command System (ICS) which it prescribes, it would be prudent to learn about it. Use its well proven structure as the basis for both your crisis response and communications. Visit the NIMS Integration Center for information and training at www.nimsc.org.

PLATFORM

Platform deals with the infrastructure your team will use during a crisis. The emphasis has been on creating Emergency Operations Centers where the team can gather and work effectively in a major crisis. There are a couple of problems with this as highlighted by Hurricane Katrina. Too often in major events from terrorism to pandemics, earthquakes to hurricanes, you can't count on your EOC surviving or your team getting to the Center. Secondly, from a communications standpoint, by the time your communication team assembles in the Joint Information Center, the story has gone around the globe multiple times and chances are the mainstream media have moved onto other stories. Your chance to participate, frame, and tell your story is gone.

The new thinking regarding crisis response and communications puts the responders into virtual control centers. There the team can assemble in minutes, rather than hours or days, because they are able to gather via the internet. As long as they can get to a place where they have the ability to login, they can participate. Web-based response management systems are becoming increasingly available. PIER (Public Information and Emergency Response) is the standard for online control centers for communication purposes and was built based on the Incident Command System and the Joint Information Center. It is used by most major oil companies, federal agencies such as the U.S. Coast Guard and numerous other organizations large and small.*

If you choose to use discreet communication tools such as Outlook for contact lists of reporters and stakeholders, email for collaborating with attorneys and outside consultants, cell phones and landlines for team coordination, your I.T. or web team for web information posting, you should be aware of the limitations. There is an increased likelihood that in the case of a major event, the basic infrastructure you count on everyday may not be there when you need it most. Additionally, the discreet tools do not lend themselves to rapid turnaround of information from drafting to publication. An integrated workflow system does speed the process when speed is important.

Clearly there is a lot to do in thinking through and preparing for a major crisis event. But often it is easy to get lost in the details. This is when it is helpful to remember that most things center on a few key elements. In the case of crisis preparedness, those elements may all start with P.

*For full disclosure purposes: your author is the creator of this system and the President of AudienceCentral, the company that provides PIER.