If an organization has done any crisis preparation, it is usually the drafting of the crisis management plan (CMP). While important, a CMP is not a magic insurance policy that protects an organization from a crisis. Nor is it a step-by-step set of instructions for what to do when a crisis hits. Laboring under either of these two assumptions will result in a rude awakening when a crisis does hit. An organization having only a CMP it has never tested is no better off than an organization with no CMP. Both will stumble and lose precious time as the crisis management clock starts to tick. This chapter examines functional CMPs and the related crisis communication system that are necessary to navigate the waves of a crisis.

THE CRISIS MANAGEMENT PLAN

The core sermon preached by crisis converts is the need for a detailed, usable CMP. It must contain the information needed to manage a crisis but should not be overly long and cumbersome. Long CMPs look nice on shelves as they collect dust but are not practical when a crisis hits (Barton, 2001; Coombs, 2006a).
Value

As mentioned previously, crises are time-pressured events where quick responses are essential. During a crisis, time should not be wasted finding needed background information, deciding who will do what, and trying to determine the sequence of events (Barton, 2001). A CMP helps to reduce response time by gathering these elements together beforehand. In addition to speed, the CMP helps create an organized and efficient response. With some framework in place, the chaos surrounding a crisis is reduced and the event is less stressful (Corporate Leadership Council, 2003). A CMP creates a system that can save lives, reduce an organization’s exposure to risks, and permit remedial actions without embarrassment and scrutiny (Barton, 1995).

Many large organizations have recognized the need for CMPs (Barton, 2001; Lerbinger, 1997). Still, in 2005 only 60% of major companies, up from 53% in 1984, have them (AMA, 2005). The numbers indicate that the message is still not being heard by all organizations. Sometimes it takes a crisis to reinforce the need for a CMP. The phrase “better late than never” comes to mind. In reality, all organizations should have CMPs because all organizations are at risk of a crisis, no matter how careful they are about their policies and operations.

Components

For CMPs, bigger is not always better. A CMP must be manageable, not filling a large binder and difficult to use. The most desirable CMP is a short document that is user friendly. CMPs can be placed in an easy to use flipchart format, bound at the top, and with each section having a different tab for easy identification. Additional format options are keeping copies of the CMP on CDs, data sticks, or on secure Intranet sites. Whatever the format, the CMP should be considered flexible and usable (Coombs, 2006a).

The CMP is, at its roots, a communication document and involves identifying who to contact and how. Contact information is provided for team members and additional experts that might be useful to the team. In fact, some crisis experts refer to the CMP as the crisis communication plan (e.g., Barry, 1984; Fearn-Banks, 2001). A crisis communication plan is a major part of the larger CMP. A CMP also includes methods and means for documenting what is said and done during a crisis. It can include reminders, in checklist form, of key actions that typically are taken during a crisis. However, it is important not to rely on a checklist for things that must be done. Each crisis is unique, and the CMP is a reference tool, not a step-by-step formula.
Following are the main components typically comprised in a CMP:

1. **Cover Page.** The cover page identifies the document as the CMP, notes that the document is confidential, provides the most recent revision date, and records the number of copies. The confidentiality statement reminds employees that the CMP should not be copied or shown to people outside the organization. Recording how many is used to control the number of copies in circulation. The revision date allows for a quick check to determine how up to date the CMP is.

2. **Introduction.** The introduction is a message typically written by the CEO. It is used to highlight the importance of the CMP and to persuade employees to take it seriously.

3. **Acknowledgment Forms.** The acknowledgment form is a removable page that employees sign and return to human resources, where it is placed in their personnel files. It is a signed affidavit saying the employee has read and understands the CMP. Having the signed documents in their personnel files encourages employees to take the CMP very seriously.

4. **Rehearsal Dates Page.** The rehearsal dates page records when the plan has been practiced and is another check on how up to date the plan and the crisis team are. Each person holding a copy of the CMP is responsible for keeping this page current.

5. **First-Action Page.** This section lists the incident commanders, how to reach them, how to activate the CMP (who should place the calls), and when it should be activated (when a situation is defined as a crisis). This section is the means of starting the crisis management process.

6. **Crisis Management Team Contact Sheet.** The contact sheet lists the names and contact information of all the members of the team, their areas of expertise, any outside consultants that may be needed, and any outside agents that may need to be contacted, such as insurance or emergency personnel. The CMT contact sheet section indicates who to contact, tells why they are relevant to a crisis, and provides a variety of means for contacting each person. This document is sometimes called the crisis directory. The CMT contact sheet provides an easy-to-use system for identifying and reaching members of the crisis team.

7. **Crisis Risk Assessment Section.** Every organization should anticipate what crises it may face. The crisis risk assessment identifies possible crises and evaluates the risk of each crisis in terms of likelihood
and impact. (Likelihood is the probability of the crisis occurring, while impact is the amount of damage [financial, structural, environmental, reputational, or human] the crisis could inflict on the organization.) The crisis risk assessment overviews the variety of crises an organization may most likely face and is not an exhaustive analysis of all possibilities. (Crisis assessment was detailed in Chapter 5.)

8. Incident Report Section. Crisis teams must keep accurate records of what has been done during a crisis. The incident report sheets are tools used to record this vital documentation. Crisis teams need this information when evaluating their crisis management efforts, and the organization needs this information when handling lawsuits or government investigations triggered by the crisis. The documentation centers on identifying when the incident was first apparent, where the crisis occurred, when various people and organizations were contacted about the crisis, and what actions were taken by whom and with what result.

9. Proprietary Information Section. While crisis managers often preach full disclosure of information, there are some policies and factual information organizations should not reveal. The proprietary information section reminds managers that certain information is confidential and cannot be released to stakeholders without CEO authorization or review by legal council (Tyler, 1997). For example, an organization should never give away trade secrets that provide its competitive edge in the marketplace without an extremely compelling reason (Barton, 2001). On a related note, an organization should never release the names of victims until family members have been notified.

10. CMT Communication Strategy Worksheet. Crisis managers must remember that communication is strategic—it serves a distinct purpose. The worksheet reminds CMT members of what it means to be strategic and to document crisis actions. Crisis managers are prompted to consider who they are talking to (the exact stakeholder), to record the specific audience to record the specific goal, to consider what they are trying to achieve with this communication goal, and to attach a copy of the actual message that was sent to the audience (Barton, 2001). Crisis managers can add other pertinent reminders that are specific to their organizations. For example, reminders about the use of specific technical terms can be added. A sample technical term reminder might describe the difference between “venting” and “releasing.” Each organization should develop its own set of additional reminders.
11. **Secondary Contact Sheet.** Stakeholders others than those listed on the CMT Contact Sheet may need to be contacted during a crisis. These stakeholders may have information the organization needs or may need to be notified about the crisis. The secondary contact sheet identifies the stakeholders to be contacted and who in the organization is responsible for communicating with this stakeholder. Stakeholder type, contact name or names, organizational affiliation (if applicable), title, contact information, and documentation (when contact was made and by whom) should be included on the sheet.

12. **Stakeholder Contact Worksheets.** During a crisis, various stakeholders will be contacting the organization. Foremost among those are usually the media, but other stakeholders may request information and need a response during a crisis. The Stakeholder Contact Worksheet section should begin with the specific procedures that should be used when a call is received (Barton, 2001). The procedures should specify where all calls should be routed and who will answer the calls. The focus typically is on identifying a spokesperson to respond to the media, a topic discussed earlier in the chapter. However, the organization should not overlook other stakeholders who may be seeking information, such as community leaders, employees, employees’ families, and investors. Although a lower priority than the media during a crisis, these other stakeholders have legitimate information needs. Neglecting these stakeholders injures the organization-stakeholder relationship. Organizations must develop procedures for all stakeholders that might contact the organization, not just the media. In addition to having clear procedures, careful documentation is essential. To record this information, multiple copies of a Stakeholder Contact Worksheet should be included in the CMP. The worksheet should include who contacted the organization, when the contact was made, the channel used to contact the organization, the specific inquiry, the response, and follow-up that was promised, and details of that follow-up.

13. **Business Continuity Plan (BC).** One organizational goal during a crisis is to resume business as usual as soon as possible. This section details what the organization will do if the crisis damages the facility or vital equipment needed to conduct business. While this plan may be a separate document, the CMP must acknowledge and recommend its use when necessary. This section should include conditions when the BC is to be used.
14. Crisis Control Center Description. When the CMP is activated, team members need to know where they should assemble. Some progressive organizations have developed special crisis control centers, sometimes called crisis command centers. Team members know to go directly to the crisis control center when they are contacted.

15. Postcrisis Evaluation Forms. Once a crisis is over, the CMT must assess its efforts. (As Chapter 9 will detail, an organization must learn from its crises.) Since the crisis management effort is primarily an exercise in communication—information collection and dissemination—the evaluation form focuses on communication (Barton, 2001; Egelhoff & Sen, 1992; Fearn-Banks, 2001). The evaluation form contains sections on the notification system used by the CMT and on its information collection efforts. The information collected through the form will help the CMT to correct weaknesses and maintain the strengths of the CMP.

Including all 15 points need not make for an excessively long CMP. However, it is a formal document as opposed to a functional one. Key points of the CMP, such as numbers 5, 6, 8, and 11, can be extracted to create a reduced version of the plan. This abbreviated version can be placed on pocket and wallet cards that all crisis team members are required to carry at all times. It is best to keep the CMP lean. If necessary, move some aspects of the CMP to a Crisis Appendix.

Crisis Appendix

Even the list of 15 elements just discussed can become lengthy. As a result, you may wish to create a Crisis Appendix to supplement the core CMP. The Crisis Appendix reflects a knowledge management aspect of crisis management. A Crisis Appendix is a crisis knowledge database that can contain precollected information, templates, and past crisis knowledge. For instance, a Crisis Appendix is an excellent place to store extended lists of potential experts and the documentation you will need for recording the team’s actions.

The Crisis Appendix can contain the supplemental or background information you might need to know in a crisis, placed in an easily accessible format. An effective way to organize this information is to think of the questions you are likely to be asked in a crisis, such as, What is your organization’s safety record? When was your last product recall? How often is maintenance performed on the equipment in question? You can store answers and information related to these and other questions. Your precollected information will reflect your organization’s
crisis risks. That means you should precollect information related to the crises most likely to affect your organization.

Templates are prewritten statements that require only a few blanks to be filled in before they are released. A number of different news releases can be drafted ahead of time and approved by the legal department. The team simply fills in the details from the current crisis, such as date, location, number of injuries, amount of damage, and so on. Time is saved, as the core message is written and approved before the crisis. Last, an organization should store what it has learned from past crises and exercises. Chapter 9 elaborates on organizational memory and learning. The idea is that the organization uses past experience to guide current actions by repeating previous successes and avoiding past mistakes. Knowledge from past crises or exercises may be useful to current crisis management efforts, so it should be available to the crisis management team.

University Application: Preparation

Do you know what to do if the building you are in right now caught on fire? Of course you get out of the building, but where should you assemble? Is there a procedure for checking in or out once you evacuate? If you do not know this information, see if you can find it. A good place to start would be your university’s Internet site. What other emergency situations should you be prepared for on campus, and how has your university prepared you for them?

The CMP Is Not Enough

The danger of a CMP is that it can provide managers with a false sense of security. Some managers feel that if they have a CMP, they are protected when a crisis hits. Three flaws challenge this assumption. First, the CMP is a general guideline for action; it represents contingencies. Crisis teams must adapt the CMP to match a specific crisis. Mindlessly following a CMP in lock-step fashion is a recipe for disaster (Fink, 1986; Littlejohn, 1983). The CMT is invaluable in adapting the CMP to contingencies and handling those factors never addressed in the CMP (Barton, 2001; Regester, 1989).

Second, the CMP is a living document. Organizations change, their operating environments change, and their personnel changes; thus, the
CMP must be updated regularly. At least once or twice a year, the CMP should be examined for necessary changes. Moreover, a crisis manager should review the CMP weekly to see if updates are necessary.

Third, a CMP has little value if it is not tested and practiced in simulations or exercises. This point cannot be stressed too strongly. Practice reveals the holes or weaknesses that must be addressed before a real crisis occurs (Wilsenbilt, 1989). For example, at an airport in Texas, a serious flaw was discovered during the crisis drill for an airplane crash. Because airport personnel had the wrong radio frequency for contacting emergency personnel in the town, their radios were worthless during the drill. This is a common problem in disaster responses and was one of many problems during hurricane Katrina. Changing the frequencies was a simple procedure, but the problem would not have been discovered without the drill. Fortunately, the drill rather than an actual crisis revealed this serious problem in the CMP. Furthermore, practice is the only way for team members to gain experience enacting the plan. Practice also builds team confidence that they can handle a crisis. The dangers of an unrehearsed team have already been addressed. Managers must not let having a CMP lull them into a false sense of security. An ongoing approach to crisis management should prevent this complacency.

Other Related Plans

Organizations should create emergency preparedness and business continuity plans that will interface with the CMP. If a crisis requires an evacuation or providing shelter-in-place, the emergency preparedness plan is in effect as well. How do the two plans coordinate with one another? This is a question that exercises can answer and can help to enable smooth coordination. Of particular concern is overlapping memberships or resource demands of the two plans. The CMP and emergency preparedness plan should complement one another and not compete in any way.

As noted in the 15 elements of a CMP, the Business Continuity Plan (BC) outlines efforts that are to be taken to either keep the organization running during the incident or to return to normal operations as soon as possible after the incident. Again, the organization should determine if overlapping membership or resource demands exist between the BC and the CMP. Also the BC and crisis teams should coordinate messages. For instance, if an alternative location is used temporarily to maintain production, workers need to be told where and when to
report for work. Suppliers and customers need to know if there will be a disruption in the supply chain, the extent of that disruption, and its estimated time span.

An excellent example of coordinating the CMP and BC is the West Pharmaceuticals plant explosion in Kinston, North Carolina. West Pharmaceuticals told customers the length of time it would take before production in their other facilities would offset the loss of the Kinston facility. Employees were told they would be working at other facilities until the Kinston facility was rebuilt. Employees were instructed where they would go and how they would be rotated home every so many weeks to have time with their families.

**PREPARATION OF THE CRISIS COMMUNICATION SYSTEM**

With the personnel and CMP in place, crisis managers must make sure the physical setup of the communication system is prepared. Elements of the crisis communication system include the notification system, crisis communication center, and online applications. Preparation entails determining if the crisis communication system is sufficient to meet the needs of the CMT and to verify that the system is operational—that it works.

**Mass Notification System**

There are times when the crisis team must send a simple message to large a number of people. This is called mass notification. Although mass notification typically involves employees, it also can include community members who need to be given safety information covering evacuation or shelter-in-place. Mass notification is done through an automated messaging system, which sends a message by phone, text message, e-mail, or a combination of these to a preset list of people. The easiest way to engage in mass notification is to outsource it. A number of different vendors, such as MessageOne, provide an array of automated messaging options. The crisis team can use automated messaging systems to inform employees that a crisis has occurred and warn the community about safety risks. The messages need to be short. Employees and community members should be told where to go to find additional information, such as a phone number, an Internet site, or an internal Intranet site for employees only. Community members should be informed of any safety risks as soon as possible. Moreover,
it is critical that employees learn about the crisis from the organization, not the news media. The mass notification system may be used whenever the crisis management process demands a short message be sent to multiple people.

Crisis Control Center

The review of the CMP noted that organizations should have a crisis control center. Such a center serves many functions: It is a place for the CMT to meet and discuss the crisis, it is an information collection center, and it is a place for briefing the media. Ideally the crisis control center is a separate area in the organization devoted solely to crisis management and equipped to meet the needs of the CMT. Large, geographically dispersed organizations should have crisis control centers at all major facilities. Multiple crisis control centers provide two benefits. First, a global company cannot expect to handle all crises effectively from one location. Extreme distances and time zone differences will hamper the crisis management effort. Second, multiple crisis control centers provide natural backups. If a crisis such as a fire or earthquake were to destroy an entire facility, the organization could use one of its other crisis control centers. Large-scale crises, such as hurricane Katrina, reinforced the need to have backups that are geographically distant from the site of the crisis. Some smaller organizations may use public relations agencies to house their crisis responses and use the agency’s facilities for the crisis control center.

To fulfill its various functions, the ideal crisis control center will have a scenario-planning room in which the CMT members can meet, a communication center for monitoring information (TV monitors, phones, computers, and wire service), and a press room for briefings. The crisis control center should be fully equipped and operational at all times. Part of being prepared is having backups for all the necessary equipment. The specific equipment will vary according to the needs of the specific organization. There must be sufficient equipment and backups for the center. The equipment must be checked regularly to ensure that it is in working order.

The crisis control center should also be stocked with food and drinks to keep the crisis team going and have administrative support to help assist it with basics tasks, such as making copies or taking inquiries. The crisis control center must have dedicated phones lines, redundant Internet access, wireless connectivity, and the ability to track the news media. It follows that IT support is essential, too (Well-provisioned, 2005).
Some crisis experts have argued that a crisis control center should be mobile or even virtual. A mobile center can be deployed anywhere. You do not have to worry if your facility is shut down, unless the mobile center was at the site of the crisis. A mobile unit would have the same equipment needs as the stationary crisis control center. The main difference is that there would be no media briefing room due to space limitations at a mobile site. However, media briefings could be handled in a separate mobile facility; rented space, such as a meeting room in a hotel; or outdoor space, weather permitting. Virtual and partially distributed teams can stay linked through wireless communication and the Internet. Even team decisions can be made through conference calls or online meetings. As noted before, the problem with virtual and partially distributed teams is the potential for equipment to fail. This risk is greatest for virtual teams because all communication is mediated. Partially distributed teams are preferable to virtual teams because you have the option to base your response from the traditional crisis communication center and to use technology to allow some team members to stay involved when they are in the field or cannot get to the crisis control center.

University Application: Crisis Command Center

Identify a location on campus that would make an excellent crisis command center. What makes that location an excellent choice? Next, create a list of all the equipment you believe should be in the crisis command center. Be sure to consider the need for backup or alternative equipment.

The Intranet and Internet

Intranets are custom-made for crises. Intranets are like the Internet but are self-contained within an organization—only organization members have access to the information, and even then, access to sensitive information is limited to those with the proper clearance (Hibbard, 1997). The beauty of an Intranet is the speed of accessing information for the CMT and other employees. The CMT can access information directly through a computer instead of through telephone calls. If the crisis team needs financial information, it can retrieve the information on the computer—no need to place a call. Collecting and analyzing information is crucial during a crisis. Crisis teams gather raw
data, transform the data into usable information (create knowledge), store the knowledge, and communicate it to others (Egelhoff & Sen, 1992). An Intranet is ideal for meeting these needs (National Research Council, 1996; Reeves, 1996). Motorola, for example, uses an Intranet as part of its crisis management efforts. It stores crisis-relevant information on its Intranet (e.g., financial and product information) and uses the system to facilitate the exchange of information during a crisis.

An Intranet allows immediate access to data about the organization; it is a place to store information, can provide a site where the crisis situation and relevant information is updated regularly, can be accessed by any employee, and allows communication to others in the organization via e-mail. Granted, not all crisis-relevant information can be collected via an Intranet. For instance, interviewing witnesses to an accident in a facility must be done in person. However, any precrisis background data needed about the organization, such as product ingredients or safety records, can be located there (for instance, in a Crisis Appendix). Moreover, e-mail and an Intranet are not always appropriate means of communicating crisis-related information to employees. Still, employee e-mail can be effective at times, and a regularly updated summary of crisis information allows employees to access what they want when they want it.

The Internet allows outside stakeholders to access your organizational information. Outside stakeholders can make e-mail inquiries or visit a Web page to access organizational information. In situations when it is an appropriate channel, e-mail can be used to reach government officials, media representatives, activist groups, stockholders, and many other stakeholders. The only limit is whether or not your target stakeholders have e-mail and you have the correct addresses. A Web page can post updated information about the crisis. Again, stakeholders have the option of deciding what information they examine and when they examine it. As mentioned, Odwalla developed a Web page when it needed to recall some of its fruit drinks in 1996. The voluntary recall and consumer communications were launched because of reports that people were becoming ill from E. coli in Odwalla fruit drinks (Nearly 200, 1996). The Web site identified the exact products under recall, how to return these products, and the reasons for the recall—the exact information customers needed to receive. Sample messages included Odwalla’s completion of the recall (November 2), an update on the recall (November 1), confirmation that the FDA found E. coli (November 4), and condolences to the Denver family whose child died from E. coli poisoning (November 8).
An organization should also create a crisis dark site. A dark site is a section of a Web site or a completely separate Web site that has content but no active links. When a crisis hits, the CMT can activate the link, and the dark site becomes accessible. West Pharmaceuticals used a part of their Web site when the Kinston facility was destroyed. BP used a separate Web site to address the deadly 2005 explosion at its Texas City, Texas, facility. A significant amount of information can be placed on a crisis site before a crisis. Such information would include background information on the facility or product, photographs of the facility (for media use), maps of the facility, and links to relevant third-party experts (Corporate Leadership Council, 2003). Specific information about the crisis can be added as it becomes known. Again, templates or holding statements can speed the posting of information. The templates or holding statements are a series of fill-in-blank statements for the media. The focus is on basic information: what happened, where it happened, the cause if known, and next steps to be taken (Business Roundtable, 2002).

Stakeholders do turn to the Web to find information about a crisis. Oddly, researchers have found that only about 60% of organizations in crisis use the Internet (Perry, Taylor, & Doerfel, 2003). The failure to use the Internet in a crisis will increasingly be a liability for organizations because stakeholders increasingly use the Internet as a means to get information quickly. If an organization does not address the crisis online, stakeholders may wonder why. There is a need to tell the organization’s side of the story, and the Internet provides an ideal place to tell that story. Unlike the news media, the Internet provides an organization unlimited space to talk about the crisis. We return to the need to tell “your side of the story” in Chapter 8.

Crisis management is moving toward using the Internet more fully. Major agencies, such as Hill & Knowlton, Ketchum, and Burson-Marsteller, feature the Internet in their discussions of crisis management client services. Their focus is on preparing dark sites for clients and monitoring the Internet for crisis-related information (e.g., Barritt, 2004). Integrating the Internet into the crisis management effort is becoming an expectation as the media and other stakeholders increasingly turn to the Internet when seeking crisis information (Lackluster online, 2002). Not having an Internet component to your crisis management effort may be viewed negatively by stakeholders.

The Internet also provides access to information outside of the organization. Some forms of external information required during a crisis can be drawn from it. In particular, government agencies provide
information on regulations and reporting procedures. Other sources might be relevant, depending upon the type of crisis being experienced. For instance, industry accident data are useful during an organization’s own accident crisis. The CMT can also monitor what is being said about the organization and the crisis in the online world, including the media and consumer-generated media. As with monitoring the traditional media, the CMT needs to know what is being said and what the stakeholders know in order to determine the accuracy of the crisis information being disseminated and if the organization’s crisis message is getting through to stakeholders. The Intranet and Internet can be valuable information processing and delivery tools when used properly during a crisis. Remember, the Intranet and Internet do not make all other information-gathering and dissemination tools and channels obsolete. Always use the channel that is most effective for the communication situation (Clampitt, 1991; Rupp, 1996).

CONCLUSION

The CMP and crisis control center complete the discussion of the six elements of crisis preparation. The CMP should be meticulously crafted before a crisis occurs. This chapter reviewed the various elements of a useful CMP. Also, the crisis communication system must be in working order. The CMP prescribes how and when to communicate during a crisis. An excellent CMP and CMT are useless if the physical structure of the communication system is not in proper working order. Calls cannot be made without working phones, and online data cannot be accessed without working computer stations. All six of the preparation elements should be reviewed and updated regularly to maintain a state of readiness for crises.

DISCUSSION QUESTIONS

1. Would you choose to have a virtual crisis team? Why or why not?
2. What are the dangers of becoming overly dependent on the Internet or Intranet during a crisis?