ELSEVIER

Corporate crisis management
Managing a major crisis in a chemical facility ☆

Steve Marwitz [a], Neil Maxson [c], Bill Koch [d],
Todd Aukerman [e], Jim Cassidy [b], David Belonger [f,*]

[a] *Formosa Plastics Corporation, United States*
[b] *CSM Solutions, Inc., United States*
[c] *Bayer Material Science, LLC, United States*
[d] *Air Products and Chemicals, Inc., United States*
[e] *LANXESS Corporation, United States*
[f] *DJB Associates, LLC, 3 Abingdon Avenue, Medford, NJ 08055, United States*

Abstract

Chemical sites should have well trained and organized emergency response plans to manage an incident within the plant or during transport. The implementation of an incident command system utilizing either internal resources or external response through mutual aid agreements is generally sufficient to address the direct impact of an event on the site. When the site resources become overwhelmed in addressing resulting issues such as press releases, medical advice/support, employees and family support, Agency notifications, etc, Corporate should be ready and able to respond.

This paper, taken from an in-depth CCPS workshop led by the author, describes an outline for corporate assistance in the event of a major incident at a site or during transportation.
© 2007 Elsevier B.V. All rights reserved.

1. Chapter 1

1.1. Background

Management of a major crisis requires prevention, planning, testing, evaluation and maintenance to mitigate and minimize the consequences. The process used by a company can determine the outcome for those affected, including employees, community and the company.

A crisis is any natural, accidental or intentional event that severely impacts people, property, and/or the environment. Effects might include fatalities, disabling injuries, significant destruction or contamination, jeopardizing the organization's reputation or products, or threatening a company's continued existence. The consequences are independent of company size, quality of management, industry or location.

A crisis could be:

- Product contamination – as experienced by Johnson & Johnson with Tylenol
- A toxic release – as experienced by Union Carbide in Bhopal, India
- An explosion – Atofina Fertilizer Plant in Toulouse, France
- A spill – Exxon Valdez

- Destruction from natural disasters such as Hurricane Katrina on the Gulf Coast and the Tsunami in Asia
- Derailment and release – Chlorine in South Carolina
- An intentional act of terrorism from outside or inside the organization, or
- Explosion and fire – BP in Texas City
- Financial

Technology and ever changing threats challenge the preparation needed to manage situations that may affect an organization's future. Minimizing risk by application of process safety management tools and security systems is an important component of an overall plan. But simply drafting a response plan that prepares for naturally, accidentally, or intentionally caused disaster or emergency scenarios is not enough. Companies must be prepared to budget for and secure the necessary resources to make this happen, provide an appropriate administrative structure to effectively manage the crisis (mitigate the consequences), and practice, practice, practice. Training and maintenance of the plan is critical to ensure that all concerned understand who makes decisions, how the decisions are implemented, and the roles and responsibilities of participants. Personnel involved in managing a crisis must be assigned their roles and be able to respond immediately and effectively.

If a major disaster occurred today, is your organization prepared to respond? If you can't answer yes to the following questions, information in this publication may help you be prepared for a major event.

1.2. Partial list of readiness questions

- Has your crisis management plan (CMP) been reviewed and approved by senior management?
- Is the CMP regularly reviewed and evaluated on a predetermined schedule to update phone lists, etc.?
- Has the CMP been communicated throughout the organization?
- Has a CM Team been appointed and do they know their role in the CMP?
- Have formal training and drills based on the CMP been conducted?
- Does the team include primary and back up assignments for: human resources, public relations/communications, environmental, health and safety (EH&S), operations, legal, IT, insurance and security?
- Has a checklist of critical actions, responsibilities and duties been developed for each function?
- Have plans and procedures been developed to respond to expected types of incident?
- Has contact information been included in the plan for the crisis management and response teams?
- Does the plan include all the information needed to manage a crisis, including internal and external contacts, databases of employees, equipment, materials, external resources, etc.?

- Have the systems and resources that will contribute to the mitigation process been identified, including personnel, facilities, technology, and equipment?
- Is the notification contact list and protocol complete and up to date?
- Has the responsibility for declaring a crisis been assigned?
- Has a crisis communications strategy been developed?
- Have arrangements been made for next-of-kin notifications?
- Can crisis counseling be provided as necessary?
- Has a designated crisis management center been identified, and does it have necessary communications equipment, including uninterruptible power supply?
- Have alternate location(s) for a crisis management center been identified?
- Have transportation alternatives to the site of the incident been arranged in advance?
- Have critical vendor and service provider agreements been established?
- Has the CMP been tested, including an unplanned drill?
- Are drills and tabletop exercises conducted on at least on an annual basis?
- Is the CMP modified as needed based on drills/exercise results?

Corporate leaders must ensure that the company, its stakeholders and the community are protected to the greatest degree possible.

1.3. Scope

A crisis management process can apply to any size company. It describes a series of interrelated processes and activities that will assist in creating, testing, and maintaining an organization-wide plan for use in the event of a crisis that threatens the viability and continuity of the organization. This publication is a tool to help organizations consider the factors and steps necessary to prepare and manage for a crisis (disaster or emergency), taking appropriate actions to protect the employees and community and help ensure the organization's continued viability. The foundation for this publication can be found in the CCPS publication titled "Guidelines for Technical Planning for On-Site Emergencies" [1]. Emergency planning is a continuous cyclical process starting with prevention and including preparedness, response and recovery. The learnings from each incident and training scenario are used to continually improve the process.

When initiating a response, it is important to insure that the goals protect the following interests in order of their priority:

- Save lives and reduce chances of further injuries/deaths
- Protect the environment
- Protect assets
- Restore critical business processes and systems
- Reduce the length of the interruption of business
- Minimize reputation damage
- Maintain customer relations

The focus of this publication is found in Chapter 2 which is divided into three parts:

(A) The planning process which provides the major elements of a CMP, including prevention, preparation and organization, and specifics including notification, assembly, team organization, and the data and procedures needed to manage a crisis;
(B) The implementation process to manage a crisis with the tools developed in (A);
(C) Training and maintenance of an effective plan.

The Appendix includes a list of definitions and information that can be used to organize a CMP.

2. Chapter 2

2.1. Planning Process

2.1.1. Prevention

2.1.1.1. Process safety management/risk management. The best response plan is one that is never used, but emergency response and crisis planning is needed because accidental or intentionally caused incidents are part of history. Frequency can be reduced by applying process safety management as presented in several CCPS publications [2–4]. Process Safety management/risk management (PSM/RMP) is the application of management principles and systems to the identification, understanding and control of process hazards to prevent process related injuries and accidents.

Successful risk management is a blend of sound organizational practices and the use of basic safety related technology. Risk management in process industries handling hazardous materials has tended toward using a multilayered approach for protective systems. Should the inner layers of safety protection fail to prevent or sufficiently mitigate the incident's effects, both on-site and off-site, then emergency response may be necessary.

2.1.1.2. Security enhancement. The primary focus of facilities that manufacture, store, use or handle hazardous chemicals has been the prevention of accidental events. After the terrorists attacks on the United States on September 11, 2001, the possibility of an intentional release with catastrophic consequences must be part of the prevention program. To address intentional acts, a security vulnerability assessment process using a risk-based approach to managing chemical plant security should be employed. One such approach was developed by CCPS and can be found in the Guidelines book "Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites" [5]. This publication provides a screening methodology to identify significant security risks among multiple sites and determine priorities for analysis of recommended changes. The methodology covers how to integrate chemical security management and process safety management strategies into a comprehensive safety and security strategy.

Security assessment should include overall warning signs and detection measures. Examples of a crisis that can have warning signs include:

- Workplace violence (erratic or threatening employee behavior)
- Activism, protests, riots
- Product contamination
- Terrorism
- Natural disasters (hurricanes, blizzards, certain floods, wildfires, etc.)

2.1.2. Preparation

2.1.2.1. Foundation. Develop a policy that specifies the role of corporate organizations in managing an incident, such as: providing field support resources to the site, role of executives (decision makers but probably not on the team), providing a buffer for the site so they can address the emergency; site reporting requirements, etc.

Policy parameters should be established in advance, such as potential pre-approval by the insurance provider of any response related contractors. Where possible, the amount of funds to help support the response team should be determined in the planning process.

A written plan with procedures to be followed when an internal or external disaster occurs should address at least the following emergency situations:

- An incident with extreme danger to life, property, and the environment.
- An incident that goes beyond the site property and can impact public health, safety, and the environment and requires large scale protective action.
- An incident that requires resources beyond those available at the incident scene, including local fire services, industrial mutual aid units, and public safety resources.
- An incident that requires resources and expertise of corporate, regional, state, federal or private organizations, especially in a kidnapping, serving of a search warrant or an incident where terrorism is suspected.
- An incident likely to generate significant questions from the media or government agencies outside the local community.

Each site in the in the company should have an emergency response plan that is compatible with the corporate plan, including team assignments, procedures and a command center. See Appendix G for an outline for a site plan.

2.1.2.2. Notification procedure. The notification process for initially contacting internal and external resources should be easy to use and efficient in establishing the degree of the emergency, the corporate response and alert to the corporate team. Some form of automated phone system to contact the team and provide information is desirable. A hierarchy of contact should be developed for use in case personnel cannot be reached. The facilities need an easy to remember central number to notify the corporate team leader. When assembly of the corporate crisis

management team is appropriate, the system should allow the team leader to notify the team with a description of the incident and instructions. The team should always have a leader in place. If necessary, an interim leader should be identified until the designated leader arrives. See Appendix E for an example.

See Appendix B for an example of a response flow chart.

2.1.3. Corporate crisis management team

It is important that an appropriate administrative structure be in place to effectively manage a crisis. Clear definitions must exist for a management structure, authority for decisions, and responsibility for implementation. Most senior managers do not have the resources to simultaneously manage a crisis and carry out normal business duties. The crisis team members should be freed of all other responsibilities during an incident. Senior managers who are not members of the crisis management team should carry on with their normal business unless requested by the team leader.

Following the incident management system (IMS) should be considered to correspond to typical plant site organization and function. The corporate team should be comprised of such functions as human resources, operations, security, legal, communications/media relations, EH&S, and distribution. The crisis management team may be assisted by as many internal support teams as appropriate, taking into account such factors as organization size and type, number of employees, location, incident type, etc. Depending on the nature of the incident, certain functions are critical for adequate support. If a person representing a critical function is not available, these duties need to be assumed by a designated backup. Another member of the team that has no immediate responsibilities could provide this backup.

The core corporate crisis management team (CMT) should include:

Team leader: The team leader, or its designate, is responsible for managing the CMT, and is the primary contact with the site or incident scene team leader. The team leader also communicates with the appropriate company executives and is usually the person that declares the emergency a corporate crisis and assembles the corporate team. The team leader assures that all team functions are covered and initiates the plan to address the emergency (see Section 2.1.3.3 below).

Ideally, the team leader should be a strong senior executive or manager who is trusted and decisive, but not impulsive and who has the authority to act without fear of being second-guessed. The manager needs a long-term perspective and should be freed from other responsibilities to lead the crisis management team until the crisis ends.

Environmental, health and safety (*EH&S*): Coordinates the EH&S response from the corporate level with the EH&S contact at the site. Should have a broad range of EH&S and product integrity experience or be able to contact appropriate experts. Arranges for dispersion modeling, provides technical advice to medical, environmental and other responders, provides data from or interpretation of MSDS, provides advice on proper protective equipment, provides disposal information, notifies government agencies and liaison with governmental agencies as those contacts are being made, etc.

Public relations: Assures accurate and timely public response is being made and is proficient in developing press releases and interfacing with the media. Coordinates media response with the site's public relations member, incorporating legal advice in communications, prepares updates for executives, arrange executive travel to the incident scene and advises the incident scene in media relations.

Human resources: Assures human relations issues are being addressed and coordinates these with the site's human resources member. Should have a broad range of HR expertise or be able to contact appropriate experts. Provides for crisis counseling, access to employee database, support in contacting family members, assembly of necessary internal and external HR resources, etc.

Legal: Provides legal counsel to the team. Coordinates with the legal coordinator at the incident scene and arranges for external legal support as needed. Participates in communication preparation and provides advice on securing incident scene for subsequent investigation.

Security: Advisor to site or incident scene team and liaison with the various agencies and security contractor(s). Provide investigative support to determine if the incident is accidental or intentional. Has a lead role in government interaction if the incident was a result of terrorism.

Team coordinator: This person or persons (could rotate this position but it is always filled) stays in the crisis center and assures the members are working with the most current information. Appointed by and assists the team leader in managing the crisis team activities including:

- Records information and comments from the team
- Makes team leader aware of new information
- Records chronological events
- Updates team members as they arrive or return to the command center
- Records questions from team members that can be used as prompts for communication between the corporate and incident scene team leader or follow-up by the team
- Assists team leader in managing CMT activities
- Tracks/documents key phone numbers, contacts, etc. that may not be predetermined prior to the crisis (e.g., hotel where site crisis team is operating during a hurricane)

Team resource (admin position)

If not a specific individual, these duties need to be assumed by one or more team members

- Provides computer support to access data and procedures
- Operates and relays fax(s)
- Provides copies of documents, such as of MSDS
- Provides weather conditions from the internet
- Gathers information that may be needed – e.g. trucking company, disaster contractor, access crisis calendar, etc. Helps to set up the room.
- Makes sure phones are ready to use.

Document control/security coordinator: (could be part of the team resource position) his position coordinates the many requests for corporate documents (from government agencies, media, etc.) and works closely with legal to facilitate distribution and protection of company assets. Should decide as part of the planning process, who will be allowed to receive specific documents.

Note: The purpose of flip charts and other notes taken during a crisis is to assist the team in managing the crisis. These notes are drafts only and are not intended to memorialize the event for any future purpose. Given how rapidly information must be processed during a crisis and how quickly information can change, it is recommended that, at the end of the crisis, all notes be condensed into a final report (reviewed by the legal department for accuracy and completeness) which will become the official record of the team response. Having done so, the draft notes should then be destroyed.

2.1.3.1. Ad hoc/support team members. The crisis management team may be assisted by as many internal support teams as appropriate. Support teams should be reassigned from existing organizations in the company and able to respond to various aspects of potential crises, such as technical support, damage assessment, site restoration, payroll, financial, and administrative support.

The following are examples of additional support for the core team:

Corporate services: Provide support for such issues as travel arrangements, secretarial help for the corporate crisis team, or communications and audio–visual support.
Engineering: Support could include assessing site damage, assisting with the planning and management of repair activities, developing options for temporary facilities and plume dispersion modeling.
Financial: Provide information as needed and coordinate activities.
Information technology: Assess system damage and activate appropriate backup systems and disaster recovery plans.
Insurance: Gather damage information and alert the company carriers
Medical: Assist in assessing the human health consequences of an event. Secure and interface with appropriate medical providers.
Supply chain: Provide administrative, logistical, and other support regarding the supply of essential materials.
Technology: Provide technical information such as toxicology. Identifies and collaborates with consultants and others with specialized knowledge of specific chemistries and exposure/contamination situations.

2.1.3.2. Databases, lists and procedures. See Appendixes C and D for a summary of procedures, databases and lists.

2.1.3.3. Initiating corporate response. A good planning process at the beginning of an incident will go a long way to provide the needed support to the incident scene team as the incident unfolds. During the initial contact with the incident scene, the team leader should:

- Establish dedicated phone numbers in the corporate command center and at the incident scene; a full-time open line should be considered
- Establish maximum time between contacts and who will make the contact
- Authorize contact between other members of the corporate and incident scene team.

The initial phase of the incident after assembling the team, the leader should:

- Ensure all the appropriate roles are filled based on the type of incident and:
  ○ Assign a team coordinator and team resource.
  ○ Account for the appropriate functions.
  ○ Make reassignments to fill gaps.
- Make plans for relief if the incident could be long term including identification of backups.
- Assure that everyone in the command center has the latest information.
- Determine how to contact anyone that leaves the command center.
- Ask each function to list possible action plan based on the information available – avoid duplication.
- List questions for the incident scene.

2.1.3.4. Crisis command center. The command center and an alternate command center should be equipped to provide for any contingency. It is best to have a dedicated room and an alternate site. If the room has multiuse, it must be available when needed. Ideally the command center should be on a UPS/backup power system. Typical equipment in the command center includes:

Phones – A primary line and at least one additional line is needed. More than three phones could result in a situation where there is too much noise in the command center. More phones in the vicinity of the command center are desirable. Ideally, phones should be set up to rollover automatically to an open line in the command center if the main line is busy.
Cell phone – At least one cell phone is desirable. It could also be used to locate team members that leave the command center.
Satellite phone – Early in an incident land lines and cell phones may experience heavy use and become jammed. Each site and the corporate center should have at least one satellite phone. *Note*: Satellite phones generally do not work inside – need line of sight to satellite.
Teleconferencing equipment – May be needed early in an incident if the team is not immediately able to assemble or to allow multiple participation in discussions.
Dedicated computer with internet and intranet access – The crisis plan and critical information for specific sites or an anticipated crisis should be on the computer hard drive and/or a web

site. Maps, weather, etc could be obtained from internet sites. Record the sites as favorites for quick access

Laptop connection(s) – Connected to a printer, the internet, etc.
Printer – Connected to a desktop and accessible to laptops.
Video teleconferencing – Useful for follow-up site communication, but probably not during the emergency.
Fax machine – Connected to a dedicated phone line.
Photocopier – Easily accessible to the command center.
TV with satellite connection – Provides ability to monitor the news.
Key office supplies – Pens, markers, flip charts, paper, etc.
LED projector
Status board
Clock - Multiple if more than one time zone is involved.
Sign in/out board – Track location of team members.

Other considerations:

- A conference table to facilitate team meetings and for review of large maps, drawings.
- Assigned work stations for each key function, plus at least one "ad hoc" station for supplemental members.
- Hardcopy backups of key site or reference information. Although potentially out of date, such hardcopy documents often are more readily accessible in the incipient stages of crisis response.

2.2. Implementation – managing the crisis

2.2.1. Initial response to a crisis – phase 1

As soon as a major emergency has been declared or identified, rapid communications is critical to mitigate the incident. The notification process must work quickly and efficiently and the initial information must be accurate and complete as possible. The call from an offsite location should come to a location that has 24 h coverage. At a minimum the initial information collected must include the callers name, return phone number and basic facts concerning the nature of the emergency. The receiver of the call must be able to make contact with the leader of the crisis team (primary or backup) within minutes of receiving the call. The call-back to the location of the incident should obtain information that includes:

- What happened?
- Has a cause been identified, e.g. accidental or intentional?
- Who is affected and what is known about those affected?
- What response is underway and who is involved in the response?

The last checklist in Appendix G contains a comprehensive list of questions that could be used to assure that nothing has been overlooked in the response at the incident scene.

The answers to these questions will allow the corporate team leader to assess the degree of involvement of the corporate team and the initial focus required of the corporate team. The next step is to provide this information to the full or selected members of

the corporate team and to develop an action plan. The contact procedure for the corporate team must allow both an alert to an incident and a method to provide the initial information that the leader obtained. The corporate team leader should prepare a short message for the crisis team and then notify the call center to immediately contact the team. The message to the team can be transmitted either by the call center or through a voice mail system. The key to an effective response requires contacting the team leader and assembling the team in "automatic" mode. The process needs to be instinctive, which only comes with practice.

A list of backups should be developed in the planning phase to insure all functions can be covered. Another approach is to assemble all primary and backup team members to assure coverage and then dismiss the backups if the function is covered. If it is likely the incident will extend beyond the current shift, the backups could be assigned relief roles.

2.2.2. Managing the response – phase 2

In the midst of an emergency, it is difficult to get all the facts, especially since the incident may be changing every minute. The situation is likely to be chaotic and fluid with rapidly changing information that is difficult to ascertain and possibly unreliable. By the time corporate is notified, there may be a myriad of Local, State and Federal agencies involved. It is important to follow the policies and procedures established in the CMP since normal company policies and procedures may hurt rather than help at first.

If there is a question about what was reported, repeat information for clarity, but try to separate fact from conjecture and opinion. This would be a good time to ask some questions even if the information isn't available. It could direct the caller to think about next steps and where help might be needed. Questions such as: "has there been any notification to government agencies?, what notification has been given to plant personnel?, what are the weather conditions?, or what is your most immediate need?" Before ending the call, arrange for the next communication and set who will make the call and the phone numbers to use.

The next steps flow from this initial information which is used in the initial communication to the team. Based on this information, the team can begin to develop some plans that would support the incident scene such as preparation to run a dispersion model, alert hospitals, begin to develop a press release, response to government information requests, etc. Based on the volume of calls and the ability of the site to manage calls it may be appropriate to set up a call center to receive calls and both provide and obtain information from callers. As part of the plan, preparation for such a call center must be made prior to any incident. Banks of phone numbers, trained operators procedures to provide a message to the operators and obtain information from the operators should be considered.

Prior to September 11, 2001, it would have been assumed that the cause of an incident was accidental. Now it is important to determine if the incident was intentional and if it cannot be determined, then proceed with the possibility that the incident scene may be a crime scene and that additional attacks at the site could occur.

It may not be possible to determine who has been affected by the incident but this needs to be a priority in early communication with the incident scene. The extent of injuries and the extent of the damage determine the business and legal issues and the communication needed. The effected parties will determine the type and priority of communication:

- If employees are being transported to local hospitals then a request for chemical effects should be anticipated.
- If there is a threat to the community then local officials must be notified.
- In environmental cases, the appropriate agencies must be notified within established time-frames.
- It is critical that all external constituents such as the general public, neighbors, customers, regulators, suppliers, vendors and contractors as well as internal constituents such as employees, shareholders and insurers be identified early in the incident. Each may require a separate but factually consistent communication. Identification of these constituents prior to an incident would significantly improve the response time.

2.2.3. Outside involvement in the response

As early as possible determine which federal, state and local agencies and responders are involved or are likely to become involved. Local contacts are best left to the site or incident scene team, but it may be helpful for corporate to begin to establish communications with the federal and state agencies. This could go a long way in freeing up site personnel to handle the emergency. If possible, all responding agencies should be directed to an identified assembly location for daily briefings.

2.2.4. Develop a plan

Each incident will require its own set of response procedures, but getting organized has some basic steps. As the team is assembling, it is important to maintain continuity of communications between the team and with the incident scene. Appendix E offers some options, but whatever is chosen, it should be communicated to the team. If the team or critical functions of the team cannot assemble in a timely manner, a virtual command center should be considered (see Appendix E). Until the team is assembled, the primary contact is between the corporate and site or incident scene team leaders. Unless the corporate team leader is within minutes of the command center it may be necessary to turn over leadership to the first team member that reaches the command center. If some critical functions on the corporate team cannot assemble in the command center it may be necessary to connect them to the command center by web or teleconference.

Once a core team has assembled, the team leader (or acting team leader) should make sure the functions critical for this specific incident are available and the team has the latest information. Each team member should announce their plan of action followed by a brief discussion to find any gaps and/or duplication. This discussion may also raise many questions for the incident scene which should be recorded and addressed in the next call to the incident scene. As new information is obtained from the incident scene, each function can adjust their plan.

One or more team members should be assigned to maintain a chronology of the event, questions raised and answers obtained from the incident scene. This person needs to act as the eyes and ears for the team leader and a source of up to date information for team members as they arrive or return to the command center

In certain crises (e.g., a severe hurricane), a site crisis management team may be unable to provide effective coordination and communication for a period of time due to local infrastructure damage and access restrictions (e.g., curfews, emergency teams only, etc.). In these situations, the corporate crisis management team may need to assume a more direct response and decision role regarding site-specific issues.

2.2.5. Crisis management team process organization chart – phase 2

See Appendix F for an example of an organization chart for the crisis management team

2.2.6. Communications

If there is a critical aspect to the management of a crisis for both immediate support of the site or incident scene team and long-term recovery for the company, it is communications. The audience is varied and may require slightly different focus and timing, but in no case should the information be "sugar coated" or minimized. Only report what you know and don't speculate. You can say you don't know and will get back to them, but make sure you do get back. Your audience may be one or all of the following:

- Employees and their families
- Customers/clients
- Contractors/vendors
- Boards of Directors
- Media
- Onsite contractors/vendors
- Government and regulatory agencies
- Local law enforcement
- Emergency responders
- Investors/shareholders
- Insurance companies
- Surrounding communities

The media is likely to be your first and most persistent audience. They will react quickly, en masse and relentlessly. The incident scene should designate a single primary spokesperson, with back-ups identified, who will manage/disseminate crisis communications to the media, responding government agencies, and others. This individual should be trained in media relations prior to a crisis. All information should be funneled through a single source to assure that the messages being delivered are consistent. The spokesperson must be available to the media and it is important that the same person continue the contacts in order to establish an ongoing relationship and continuity. A spokesperson from the site will generally understand the com-

munity and its issues and will be more likely to have credibility versus a representative from Corporate. Be aware that company history will be fair game including any government actions, the environmental record at any site and activist allegations. It is possible, especially for an incident off-site, that the official spokesperson will not be a company representative. All communication should be cleared through or made by the official spokesperson.

It is important that the company spokesperson at the scene coordinate with corporate communications. Support from corporate in preparing the press release is critical to avoid misstatement, especially for the initial release. The CMT may have knowledge of issues or concerns unknown to the scene person. This will also give the Legal Department a chance to review the release. Early in an event there is limited information so the questions can be collected and used for a later report.

Some hints in your communication plan:

- The initial release should be developed and distributed quickly. Consider using the internet and intranet. Communications should be timely and honest.
- Regular, detailed situation update information sharing is critical. Let the audience know the timing of the next update.
- Responsiveness to regulatory agencies and government officials is critical.
- Help agencies or officials communicate to media and public:
  ○ Set up daily briefings at a designated location.
  ○ Consider joint news releases or media interview opportunities.
  ○ Consider community meetings.
- Exert control over the story, guide media on story angles.
- When possible, provide information before being asked.
- Do what it takes to be responsive.
- Speak directly to the public whenever possible.
- Let them vent their anger, fear and frustration. This is painful, but necessary.
- Assume no event at a plant is a small story.
- Don't underestimate the level of interest about the plant.
- You can't hide anything, so don't try.
- Relationships built during earlier phases of the incident pay dividends.
- To the extent possible, an audience should hear news from the organization first.
- Communications should provide objective and factual assessments without conjecture.
- All employees should be informed at approximately the same time.
- Drafts of message templates, scripts, and statements can be prepared in advance in generic terms.
- Provide technical resources for the public relations representative to assist then in answering technical questions.
- Communicate in a manner appropriate to circumstances:
  ○ Face-to-face meetings (individual and group)
  ○ News conferences
  ○ Voice mail/email
  ○ Toll-free hotline

  ○ Special newsletter
  ○ Announcements using local/national media.

2.2.7. Immediate aftermath and recovery – phase 3

In situations where the CMT had to assume a more direct leadership role for site issues (e.g., the hurricane example), site-specific decisions typically are returned to the site crisis team during this phase.

The assessment and business recovery begins as soon as the emergency is stabilized. If the emergency is considered a crime scene, legal advice is essential to maintain the integrity of the investigation. As the investigation proceeds the information flow will improve and more and more reliable information will become available. Communication of new or revised information should be discussed with the corporate crisis team before it is released to both confirm the information and avoid confusion. It is likely that rumors, blame and false reports will already be circulating, making the timing and content of communication of the revised information critical.

In the days and weeks following the incident the long-term effects will become more obvious and details and fact will emerge. Blame will likely come from many sources and effective, not reactionary communication, will be critical. The audience for subsequent communications will be as broad as initial communication, including company personnel, the community and authorities. Appropriate members of the corporate crisis team will likely be involved in the communication effort many days and possibly weeks following conclusion of the incident

2.3. Training and maintenance

2.3.1. Training

The crisis management teams should be educated about their responsibilities and duties. Checklists of critical actions and information to be gathered are valuable tools in the education and response processes. CMT members should be trained at least annually and new members should be trained when they join. To extent practicable, the team leader should receive additional training in appropriate emergency and crisis response, such as HAZWOPER incident command.

Training should include testing and practice. The scope of testing should be designed to assess the level of understanding of the participants. Also, training should be reinforced through practice drills of various sizes and complexities up to a full-scale activation of the CMP, including external participation by public safety and emergency responders. Initially, tests should start out relatively simple, becoming increasingly complex as the test process evolves. Early tests could include checklists, simple exercises, and small components of the CMP.

2.3.2. Maintenance

A plan is only effective if it is current and practiced. Keeping a plan current is an ongoing task that needs constant attention. Obviously phone numbers require the most vigilance and could be tied to a database for easier maintenance, but there is other

information that must be tracked. Contact information for external contacts and procedures are likely to change. An effective method of providing current information is to apply ISO type document control procedures.

Access to the information is also important. The team information could be stored on a server or accessed from an Intranet web site. In either case someone must be responsible for keeping the information current. Since access to the information is critical, the information should be available from a remote location.

Appendix A. Definitions

Asset – Any person, environment, facility, material, information, business reputation or activity that has a positive value to an owner.

Consequence – The direct negative result of an event, usually expressed in terms of the magnitude of that area over which these impacts occur.

Contact list – A list of corporate and site team members and other key personnel in a crisis. The list should include phone numbers (home, office, cell phone), email address, etc.

Crisis – A crisis is any natural, accidental or human caused event that severely impacts people, property, and/or the environment. Effects might include fatalities, disabling injuries, significant destruction or contamination, or jeopardize the organization's reputation or products, threatening a company's reputation or its continued existence. The consequences are independent of company size, quality of management, industry or location.

Crisis management – Process used before, during, and after an event to resolve the crisis, minimizes loss and downtime or otherwise protect the organization. The ability for fast decision making is essential.

Crisis management center – A location equipped with appropriate equipment for team members charged with commanding, controlling, and coordinating a response to a crisis.

Crisis management planning – An ongoing proactive process supported by senior management to ensure appropriate actions are taken to analyze the impact of crisis events and provide overall coordination of the organization's timely and effective response to a crisis.

Crisis management team (CMT) – A group appointed by senior management to support incident/event response. Usually comprised of personnel from such functions as human resources, operations, security, legal, communications/media relations, EH&S and distribution.

Disaster recovery – Actions to minimize further losses from a disaster and to begin the process of recovery and return the organization to an acceptable condition.

Emergency – A combination of events or circumstances that results in loss of an asset whether it is loss of capability, life, property or equipment and demands immediate action and intervention to minimize potential losses.

Exercise/drill – An activity for the purpose of training and conditioning team members and personnel in appropriate crisis responses with the goal of achieving efficient performance during a crisis.

Incident management system (IMS) – An organized system of responsibilities and standard operating procedures used to manage and direct emergency operations.

Mutual aid agreement – A pre-arranged agreement developed between two or more entities to provide for assistance to the parties of the agreement.

Prevention – Processes to avoid a crisis occurring. The tasks should include compliance with corporate standards, application of risk management processes and programs.

Recovery – Plans and processes to return an organization to normal operations or to reconstitute operations to a new condition. Recovery steps should include damage and impact assessments and prioritization of critical processes to be resumed.

Response – Executing the plan (perform those duties and services) to preserve and protect life and property. Response steps should include notification, situation assessment and plan execution including communications, and resource management.

Risk management – The systematic application of management policies, procedures and practices to the tasks of analyzing, assessing and controlling risk in order to protect employees, the general public, the environment and company assets while avoiding business interruptions.

Shelter-in-place – The process of securing and protecting people and assets in the vicinity of a crisis.

Tabletop exercise – Training that presents a limited simulation of a crisis scenario in a narrative format in which participants review and discuss, not perform, the response plan including: methods, procedures, coordination, and resource assignments associated with the plan.

Appendix B. Example of a crisis management process – flowchart
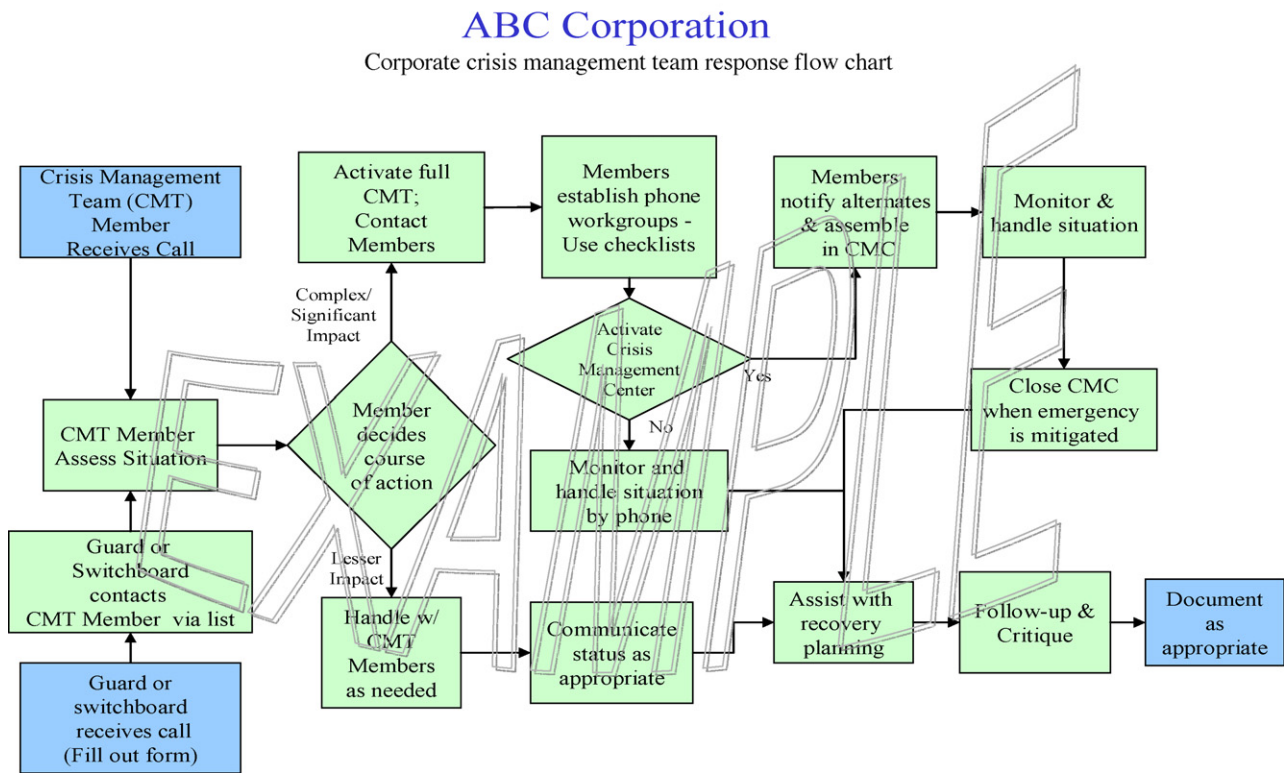
Appendix C. Suggested lists and databases

Plant database for all facilities – easy reference for the products, services, purpose and some facts about the facility
Bomb threat guidance
Crisis management team (CMT) roles
CMT checklist by function
Conference call (teleconference) procedure
Corporate command center location and equipment description information
CMT contact procedure
CMT members and backups – list
HR contacts – list
Disaster contractors – list and contact procedure
Dispersion modeling – how it arrange for modeling
Employee emergency contact procedure
Senior executives contact list
Financial division contact
Central emergency reporting processes
Insurance carriers – list and contact procedure
Language line translation services
Lawyers – inside and outside
Procedure to staff bank of 800 phone numbers
Product recall procedure
Reimbursement and continuation of payroll policy
Site crisis teams and information
Talking points on security and crisis management
Transportation security administration contact protocol
Government agencies – contact numbers
Voice mail procedures
Search warrant checklist
Kidnap and extortion plan
MSDS

Company directory
Weather service
Site maps or drawings
Employee database
Air service and security consultants – list and contact procedure

Appendix D. Suggested procedures

- Defective product
- Weather emergency – tornado, hurricanes, freeze, flood
- Notification of families
- Media protocols
- High jacking
- False accusation
- Travel restrictions
- Evacuations – International SOS

Appendix E. Initial planning

E.1. Team leader continuity

When the team leader decides to assemble the team and the team leader is not in the corporate command center (or not close to the command center), the team leader needs to consider how to get to the command center while remaining available to the site. There are two options and the team leader should include the option in the notification to the team.

The team leader sends a message to the team with the initial information and instructions about assembling for the incident. This information will include instructions for the first team member arriving at the command center to call the team leader.

The team leader will maintain contact with the site of the incident until contacted by first member arriving at the command center (now the interim team leader).

The team leader will update the interim team leader including name and phone number of the site contact. Contact the site with the name and number of the interim team leader and proceed to the command center.

OR

Team leader proceeds immediately to the command center. The team leader sends a message to the team with the initial information and instructions about assembling for the incident. This information includes information that the team leader is enroute to the command center and can be contacted by cell phone (provide number). The team leader provides the site with

a cell phone number if there is a need to make contact before arriving in the command center.

E.2. Virtual command center

If it is not possible for the team to assemble in the command center in a timely manner, a virtual command center with the team connected via computer and teleconference provides a reasonable substitute for a face-to-face command center. A predetermined teleconference number, remote access to the company's database and an electronic method to share information is needed to make this effective. The biggest challenge is finding a system where documents can be shared on-line to provide information, updates, action plans and status as would be provided in a physical command center. A system like Microsoft's [TM]SharePoint could provide this connection.

Appendix F. Example of crisis management team organization
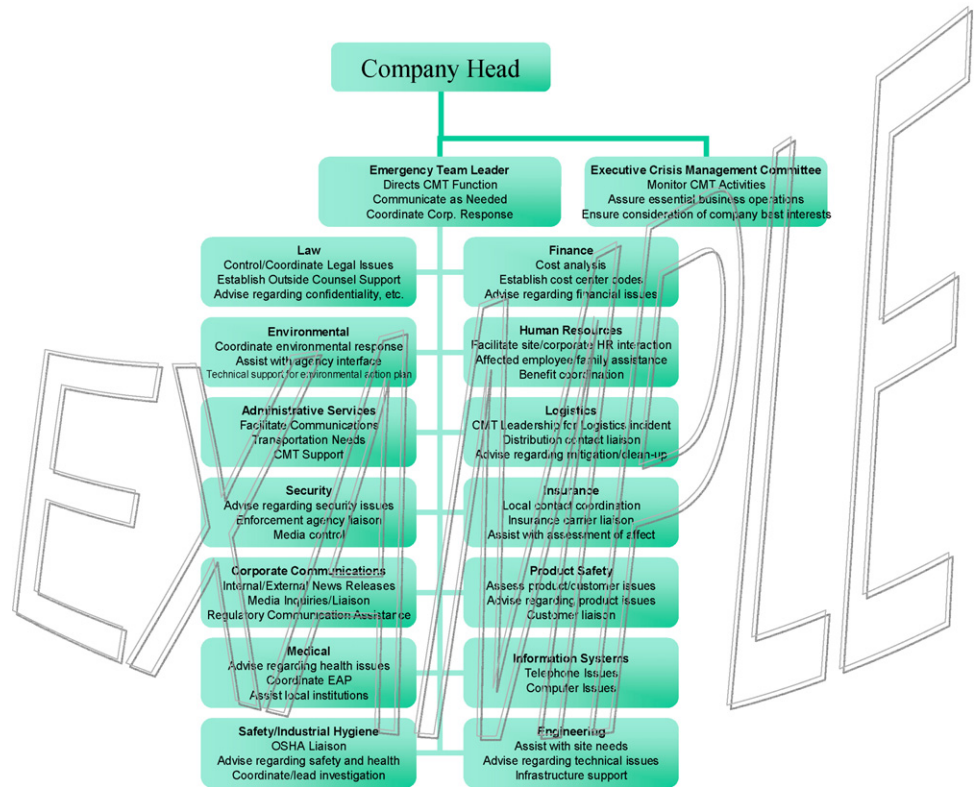
Appendix G. Site plans

G.1. Site crisis management

G.1.1. Introduction

This outline could be used by site managers to assist in developing plans to protect anyone inside the site and the public in the vicinity of the site. Effective planning and response is achieved by coordination, cooperation and participation of many groups, individuals and the community. Each site should have a crisis management plan and a team identified to carry out the plan. This plan should be communicated to all employees on the site and reviewed on a periodic basis. The plan also should be tested in a drill on a routine basis.

Many of the same procedures, command center equipment and team roles as described in the corporate system apply to the site. See Chapter 2 for these details.

G.1.2. Elements of the site crisis management plan
G.1.2.1. Site manager responsibility – direct and delegated .

- Assess the natural and human caused risks and make appropriate resources available.
- Primary contact with corporate
- Coordinate the plan with municipal or LEPC officials to ensure compatibility
- Assign appropriate site staff members to the site crisis team with defined responsibilities
- Conduct drills and initiate plan revisions based on drill evaluations.
- Conduct periodic safety checks of the physical site and equipment
- Provide copies of the disaster plan to the Local Emergency Planning Committee (LEPC)

G.1.2.2. Plan basics . A written plan with procedures to be followed when an internal or external disaster occurs. The plan should:

- Identify and address the unique needs of the site's occupants and hazards.
- Should address at least the following emergency situations:
  ○ Fire and explosion
  ○ Severe injury(s)
  ○ Utility failure
  ○ Release of hazardous materials
  ○ Acts of terrorism or civil unrest
  ○ Severe weather situations
  ○ Health Crisis (SARS, Avian Flue, etc.)

G.1.2.3. Plan specifics.

- The plan procedures should address, as a minimum:
  ○ Assignment of responsibility to staff members
  ○ Special needs of affected individuals
  ○ Notification of local emergency services
  ○ Request for outside assistance
  ○ Provisions to shelter people inside the site if it's more dangerous to evacuate
  ○ Evacuation plans if it's necessary to leave the site
  ○ Arrangements for transportation if it is necessary to evacuate to a remote location
  ○ Protection of valuable records
  ○ Other site specific issues
- A description of how site management will notify the crisis team and site occupants of an actual or impending disaster/emergency
- A list of emergency telephone numbers, including the crisis team, emergency responders, community and agencies
- An identification of designated shelter areas or best protective areas inside the site
- An identification of evacuation assembly areas outside of the site
- A list of responsibilities and assignments(s) of staff members for anticipated emergency situations
- A description of education, training and drills required to assure effective operation of the plan
- Specify who will be in charge (with an alternate) and where that person will be positioned. The crisis management center should have adequate communications and an alternate location should be designated in case an evacuation is needed.
- Provisions for use of the control system called the "incident management system (IMS)." IMS establishes who is in command and breaks each unit into sections or divisions so each leader has a manageable span of control. In some situations, the incident commander may need a site representative as part of a unified command.
- A provision for periodic review and revision.

G.1.2.4. Plan recommendations. The ideal plan is easy to find and easy to read during an emergency. The plan must be specific enough to give directions for immediate action, but flexible enough to allow for changes as unexpected situations develop.

A few hints to consider are:

- Step-by-step procedures should be as simple as possible so that they are clear to someone unfamiliar with the plan.
- Whenever possible, save time and avoid confusion by developing standard procedures for various situations that rely on consistent action as much as possible.
- Crisis team responsibilities should be as close as possible to normal jobs so team members are familiar with their emergency location and responsibilities.
- Use checklists to ensure that infrequently practiced emergency jobs are done correctly.
- Arrange for mutual aid agreements
- Consider a community alert system (siren or automatic phone notification)
- Be aware of the history of natural or man-made disasters which have affected the site and community when planning notifications and responses.
- Understand the general weather and climatic patterns of their area.

- Provide street maps to assess vulnerability to hazards and evacuation routes.
- Provide site and building plans so that shelter areas can be determined and evacuation routes planned to avoid hazardous areas (boiler rooms, etc.) and take advantage of safety construction (fire walls, etc.).
- Organizational charts showing responsibilities associated with job titles and list names, titles, addresses and phone numbers of key personnel. During emergencies, the charts, prominently displayed on a wall, provide the necessary information at a glance.
- Provide a pocket card to the team listing key information for quick reference.
- Assign recordkeeping duties in the crisis team
- Provide media training for the site manager and a backup

G.1.2.5. Training and drills. Training and drills are essential to having an effective response in times of an emergency.

- Training for each team member in their emergency role should be required and supplied by the site. Instruction should be given as part of an on-going training program.
- Exercises, drills and tests should be utilized for training once the team has been trained as in the procedures to follow and their respective roles.
- Conduct drills at various times during the year to account for seasonal differences

G.1.2.6. Site checklist. The checklist assumes the activation of the site crisis management team:

- What is the status of arrival of a representative for each function? Who will cover missing functions?
- What is the status of the site crisis management team? Who or what function is missing?
- Is a dispersion model needed? Has it been run?
- Was the incident the result of terrorism or a security breach? What are the appropriate actions?
- Are there sufficient resources on site? What/who is needed for support?
- What outside response teams are on site?
- What notification has been made to outside agencies? What is required?
- Have appropriate internal notifications been made as listed in the notification procedure?
- What is known about the site impact?
- Has a headcount been taken and what is the status of employees and contractors?
- If there are injuries, has the local Employee Assistance Plan or Corporate HR been put on notice to standby (or arrive) for support?
- If anyone was injured and they cannot call home, are there assignments to make the contact for the employee?
- Who is the on-scene incident commander?
- Has the local community advisory committee been notified of the event?
- Has the emergency scene been secured/protected so evidence needed in an investigation isn't corrupted?

- Do we need a place for families of employees to gather?
- What is being done about communication within the company—voice mail or email status updates? Who is responsible to do this?
- Are local hospitals able to handle the number of injuries and technical (exposure) issues? Do we have someone assigned as a direct link to each hospital involved?
- Has an outside clean-up company been notified—what is their response time?
- Is there an investigation underway? Are people involved identified and are they being interviewed? Is legal counsel involved in any interviews? Is Legal Counsel needed in the investigation?
- Is a press briefing being arranged? Who is coordinating? Where will it take place?
- If there was a community evacuation, is there an assigned location for residents to assemble? Has a headcount been taken and what is the status?
- Is there a need for food, relief, etc. if this will be more than a few hours?
- Are there resources to handle secondary effects of the incident? Is water run-off from fighting a fire being contained? Is evaporation from a spill being suppressed or contained?
- Is this event impacted by any recent regulatory changes? (Question for EHS professionals and legal counsel.)
- Are employees from the site affected and other management up to date on the status of the event?
- Are medical files of employees at the site immediately available as needed?
- Are there arrangements for disposal of contaminated materials? What are the legal requirements of such disposal?
- Does the site need to move the command center to a remote site? Is there a remote site equipped to handle the communications?
- Does purchasing need to be called in to help with vendors/contractors?
- Is there a landing pad nearby for medivac?
- Is there a need to shut down utilities/pipelines entering the site?
- Is there a need for a post event debriefing/counseling, especially for emergency response people involved in rescue?

References

[1] *Guidelines for Technical Planning for On-Site Emergencies*, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, 1995.

[2] *Guidelines for Integrating Process Safety Management, Safety, Health and Quality*, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, 1996.

[3] *Guidelines for Implementing Process Safety Management Systems*, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, 1994.

[4] *Guidelines for Process Safety Fundamentals in General Plant Operation*, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, 1995.

[5] *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, 2003.