THE BUSINESS ROUNDTABLE'S

POST-9/11 CRISIS COMMUNICATIONS

toolkit

Best Practices for Crisis Planning, Prevention and Continuous Improvement

JUNE 2002

Table of Contents

Executive Summary

"Crisis planning and preparedness is not a back burner issue anymore. It cannot be at the tail-end of our annual list of priorities—either yours or the federal government's."

Governor Tom Ridge
Director of the Office of Homeland Security
April 8, 2002

The following *Crisis Communications Toolkit* is a product of The Business Roundtable provided to its members. It is designed to enable members of the BRT to tailor for their own unique purposes a workable post-9/11 crisis communications plan that includes crisis preparation, prevention, and continuous improvement.

Please note that while the focus of this document is on crisis communications, references are made throughout the document to crisis management as some companies house crisis management responsibilities within their communications departments. It should also be noted that the threats that cause crisis situations are not limited to physical "plant" facilities, but also include cyber attacks that may have a profound impact on the delivery of goods, information and people either by the private or public sector.

Overall, this toolkit:

- Equips companies with the most effective communications infrastructure in the event of a crisis. Having the most effective crisis plan will enable the business community to be more fully prepared in the event of a crisis, and to work

effectively with the Office of Homeland Security; federal, state and local law enforcement; and other members of the business community. This plan links directly to the Roundtable's CEO COM Link (see Using CEO Com Link, Part 1: Role of CEO COM Link) and to other tools under development by the Roundtable.

- Identifies crisis communications Best Practices and presents them to Roundtable members in an easily adaptable format. Many of the Best Practices described in this document may already be part of some member plans, while some Best Practices may offer enhancements to member plans. While the information may provide added value for general crisis planning, this information is especially targeted to a worst-case situation, such as a terrorist attack. Decisions to deploy any of these Best Practices are at the discretion of individual companies.

This document is based on experiences and observations in the handling of a wide variety of crises; and pays particular attention to the lessons learned from 9/11 and ideas submitted by members of the Roundtable. It is important to note that particular emphasis is placed on crisis prevention, communication of risk and the use of emerging communications tools, such as CEO COM Link.

By all measurements, the events of 9/11 and the continued threats to security and global business have changed the way we think of crisis preparation, prevention and response. As a guide or clearinghouse of Best Practices—for inclusion in or adaptation for your company plans—this toolkit should be shared with your vendors, subsidiaries or suppliers so that everyone in your supply chain is as prepared as possible.

It is useful, particularly in the aftermath of the events of 9/11, to review the cycle of a crisis:

Phase 1: Pre-crisis, which describes the state of readiness, protection and prevention any organization may be in. The characteristics of this phase in a Best Practices sense include continuous improvement of all aspects of planning and training; and a vigorous communications program which encourages the identification of vulnerabilities and early warnings.

Phase 2: Crisis, which involves the rapid response to a crisis, calling upon all the resources that have been put into place during the pre-crisis phase. Inherent in this phase is a communications process that recognizes the interests of all stakeholders (e.g., employees, the public, investors, communities, etc) and the effective messages that convey concern for those who may be affected, a commitment to solutions and clear explanations of actions underway.

Phase 3: Recovery, which may vary in length of time and includes all the aspects of restoring normalcy to operations as well as to reputation should a company's reputation be tarnished. This period, which is centered on effective communication, may include advertising, philanthropic efforts and above all a constant flow of information on the recovery process.

BEST PRACTICES

Several Best Practices were reinforced or have emerged due to the events of 9/11 and continuing concerns about terrorism. Crisis communications experts recommend that companies:

1. Establish a Full-time Commitment to Crisis Management.

Coordination of the crisis management and communications function—which in many cases is an add-on responsibility shared among corporate communications, security, legal and other departments in corporations—now calls for full-time commitment by at least one senior staff member with authority to keep the process alive in every respect—including training, prevention, crisis response and recovery.

2. Employ Communications Techniques to Maximize Crisis Prevention.

The best crisis is the one that never happens—and the odds of preventing a crisis increase as several coordinated communications techniques, including 24/7 telephone hotlines, email and other programs become part of an enhanced culture of listening for early warnings. In addition, companies should identify and build relationships with representatives of relevant local and federal agencies.

3. Designate Backups.

Redundancies in staffing and infrastructure are both important. Preparing for infrastructure breakdowns or failures is crucial, as is backup for personnel. On the staffing level, including the CEO and senior management level, it is especially important to designate backups in the event an individual is not available; and also to

provide for relief should a crisis run for a long period of time. On the infrastructure level, designating several backups is crucial in order to allow for continuity in the event of destruction or breakdowns. Establishing backups is particularly critical given the widespread reliance on electronic communications, including voicemail, email and networked communications.

4. Keep Vendors and Consumers in the Loop.

Crisis plans should extend beyond the boundaries of corporations to include procedures for vendors and customers—vital parts of the entire chain—with key stakes in early warnings and prevention, as well as in emergency response.

5. Address Terrorism as a Global Concern.

Recent history has shown that the global components of U.S.-based companies are vulnerable. For this reason, all aspects of crisis plans should be considered global and should involve all locations. Specifically, it is important to "drill down," or indoctrinate, all locations with:

- The basic plan with notes on how locations are to communicate with headquarters at the first signs of a crisis.
- The tools to localize the plan.
- The guidelines on managing the crisis locally if communication with headquarters breaks down.

6. Be Sensitive to the Communication of Risk.

Security threats, exacerbated by very real feelings of a lack of control, raise high levels of fear among everyone. Research has aided in development of guidelines for Risk Communications. It advises against using probability statistics or unrealistic comparisons; and

emphasizes expressions of concern, candor, and explanations of actions.

7. Understand the Pros and Cons of the Web.

The Web is an important tool on both sides of the terrorism equation. It is a tool by which business can communicate, train, store and retrieve data as never before, but it is also a tool used by terrorists for the same purposes—with the added high vulnerability that they can impede, hack into or destroy systems. Companies should take steps prior to a crisis situation to ensure the safety and security of their networks and electronic communications systems.

DEFINING IMPORTANT TERMS

In order to clarify the use of commonly used crisis management and related terms, the following list of definitions may be useful.

Best Practice:

Best Practices are those accepted management or communications tools or processes that are effective in a specific concept or significant detail. A Best Practice generally is innovative, and is a particularly reliable or valuable enhancement.

CEO COM Link:

A tool through which BRT CEOs can efficiently communicate in the event of a major national crisis. Provides a means for information sharing among companies, and between companies and the Office of Homeland Security or other relevant government bodies. CEOs must register and be credentialed before they can gain access to this crisis tool, and will receive separate instructions on using the system.

Crisis:

A major event, generally characterized by one or more of the following:

- Possible or actual harm to individuals or property, including computer networks
- Imminent threat to "business as usual"
- Imminent threat to company or brand reputation
- Media attention—either immediate or potential

Crisis Communications Plan:

The communications elements of the larger Crisis Management Plan, which details communications guidelines for crisis prevention, management and recovery.

Crisis Management Plan:

The plan, which encompasses the management structure, crisis communications plan, responsibilities, and infrastructure and procedures needed to support management in crisis prevention, management and recovery.

Emergency:

A situation, which is localized and controllable, such as a fire or accidental injury. It generally is characterized by one or more of the following:

- Local media attention.
- No substantial or uncontrollable threat to individuals or property.
- Little or no disruption to operations.

- No threat or indication of problem beyond the specific location.

GETS Cards:

Government Emergency Telecommunications Service (GETS) cards provide priority telephone connectivity to parties considered by the federal government to have a role in addressing issues related to homeland security. Cards enable BRT CEOs to gain access in a crisis to potentially congested phone lines at the time of a CEO COM Link call.

Issue:*

A controversy, generally characterized by:

- Early warnings through any number of sources—e.g., activist groups, legal claims, government investigations, research announcements, etc.
- Sufficient time to develop strategies and steps which may solve the problem before it escalates to a crisis.
- No immediate harm or disruption to business.

* AN ISSUE IS NOT A CRISIS.

Third Party:

An organization or credentialed, respected individual outside the company, who has a specific perspective on an aspect of the organization or situation—and is willing to express this perspective publicly.

Notes:

Notes:

Understanding and Applying the Government's Risk / Threat Advisory System

The Office of Homeland Security has released a five level, color-coded threat advisory system which establishes definitions for assigning the threat condition to an area of the nation, a city or community; or even an individual government or major private sector facility. The Homeland Security Advisory System's (HSAS's) assigned threat level will determine what protective measures should be undertaken in order to reduce a location or facility's vulnerability to an attack.

In light of the attacks of 9/11, some companies are also considering or beginning to adopt a threat advisory system to effectively communicate risk-related or crisis preparation information to employees and vendors. The Roundtable intends to work closely with the Office of Homeland Security to further explore how the business community could effectively develop advisory systems that are complementary to the HSAS. The BRT will also explore how information can be shared, in particular the communications protocols that correspond to each level of threat.

The Office of Homeland Security defines its Advisory System levels as follows:

Low Condition - Green

Low risk of terrorist attacks. The following Protective Measures may be applied:

- Refining and exercising preplanned Protective Measures
- Ensuring personnel receive training on HSAS, departmental, or agency-specific Protective Measures; and
- Regularly assessing facilities for vulnerabilities and taking measures to reduce them.

Guarded Condition - Blue

General risk of terrorist attacks. In addition to the previously outlined Protective Measures, the following may be applied:

- Checking communications with designated emergency response or command locations;
- Reviewing and updating emergency response procedures; and
- Providing the public with necessary information.

Elevated Condition - Yellow

Significant risk of terrorist attacks. In addition to the previously outlined Protective Measures, the following may be applied:

- Increasing surveillance of critical locations;
- Coordinating emergency plans with nearby jurisdictions;
- Assessing further refinement of Protective Measures within the context of the current threat information; and
- Implementing, as appropriate, contingency and emergency response plans.

High Condition - Orange

High risk of terrorist attacks. In addition to the previously outlined Protective Measures, the following may be applied:

- Coordinating necessary security efforts with armed forces or law enforcement agencies;
- Taking additional precaution at public events;
- Preparing to work at an alternate site or with a dispersed workforce; and restricting access to essential personnel only.

Severe Condition - Red

Severe risk of terrorist attacks. In addition to the previously outlined Protective Measures, the following may be applied:

- Assigning emergency response personnel and pre-positioning specially trained teams; Monitoring, redirecting or constraining transportation systems;
- Closing public and government facilities; and
- Increasing or redirecting personnel to address critical emergency needs.

Notes:

Consider how your company might act under the threat levels issued through the Homeland Security Advisory System.

Low Condition—Green

Guarded Condition—Blue

Elevated Condition—Yellow

High Condition—Orange

Severe Condition—Red

Notes:

Knowing and Understanding Specific Audiences

In a homeland security crisis, audiences have unique and immediate communication needs. Consider the following overview:

The Public Should Receive:

- Calm assurance that all resources, public and private, are being deployed to protect everyone. In many cases, this will include important information on redundant or backup resources.
- Survival information for those immediately affected.
- Preparatory survival information for those who may be affected.

Employees (Worldwide) Should Receive:

- Survival information and assistance for themselves and their families.
- Information on when, if and how to report to work; and how their jobs and workplace may be affected.
- Information on where to receive situation and status updates.

Customers Should Know:

- If and when products will be received and services rendered.
- Whether there are, despite all precautions, any risks involved with consumption or use of the products or services.
- What they can do to eliminate or reduce risk.

Government Should Know:

- What the business community can do to help.
- What emergency assistance is needed to continue essential business activity.

Capital Markets Should Receive:

- Assurances that finances are secure.
- Assurances that insurance resources are sufficient.

Companies in the Same or Allied Industries and in the Affected Community Should Receive:

- A prompt briefing on what has happened so that they can assess their own threat levels.

CEOs Should Receive:

- Information to make decisions for the protection of employees, customers, vendors, affected public and facilities.
- Information on how best to help those in need.
- Information on next steps or precautions to take.
- Information and strategic advice on preserving company reputation and investor confidence.

Notes:

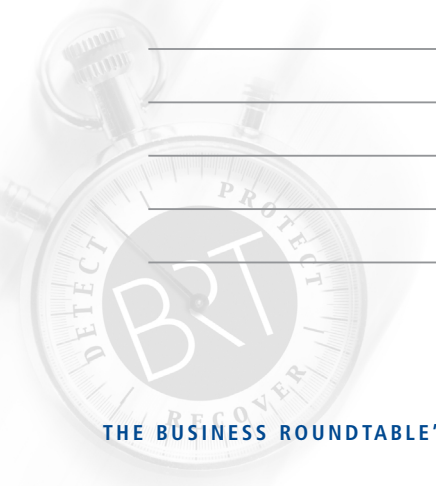
List particular national, state and local audiences that are of importance to your company in times of a crisis:

National

State

Local

Notes:



Assessing Your Crisis Plan

To assess your company plan, the following brief scorecard may provide a useful benchmark. This is not a pass/fail effort; it is simply a tool to focus on where your plan stands in terms of its utility. While it may be interesting to average the score for the entire plan, it may be most useful to examine the scores for each category, thus helping to create a set of objectives for improving the plan. This assessment tool can also be employed to assess the status of your plan on a quarterly basis.

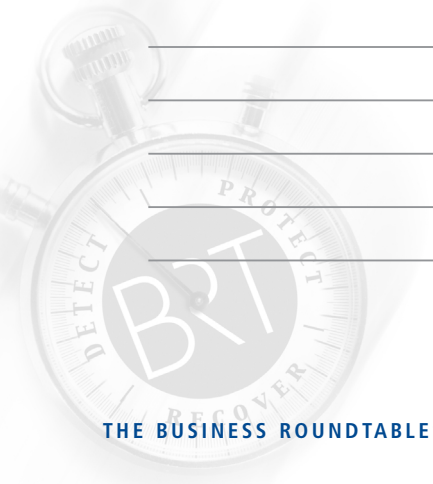
In order to achieve some level of objectivity, this assessment should be conducted by someone familiar with crisis communications and management, but not historically responsible for creating the plan or administrating it. This individual could be a new member of the communications staff or an outside consultant brought in for the evaluation process.

Rating System—Consider the following scale: **1** Poor—difficult to use (e.g., topic is not covered or is not included or plan is not sufficiently clear or comprehensive, **2** Fair—somewhat cumbersome or dated and requires editing and additional materials, **3** Good—effective for practical purposes, but could be improved somewhat, **4** Excellent—could serve as a model or Best Practice example, **5** Innovative—meets criteria of # **4**, but also includes one or more innovative approaches

	1	2	3	4	5	Changes/Additions	Responsibility	Deadline
Clarity of your plan: Is it:								
• Concisely written?								
• Well organized?								
Scope of your plan: Does the plan cover the basics?								
• Procedures for first response/crisis investigation and determination								
• Team and responsibilities								
• Functional checklists								
• Notification system								
• Headquarters' responsibilities/ remote or division responsibilities								
• Crisis site or "GO" teams								
• Spokesperson designation								
• Key message guidelines								
• Media tips								
• Communicating risk								
• Media monitoring								
• Dark Website and other Web procedures								
• The dedicated crisis room: logistics, maintenance and security								

	1	2	3	4	5	Changes/Additions	Responsibility	Deadline
Timeliness of your plan: Does the plan include current provisions that reflect:								
• Web-based Technology								
• Post 9/11 Concerns								
Prevention techniques in your plan:								
• Does your plan address prevention with detailed techniques and programs?								
Practice techniques in your plan:								
• Do you conduct a crisis simulation at least once a year?								

Notes:



Developing or Updating a Crisis Communications Plan

Crisis communications plans have evolved over recent years from the post-Tylenol prototypes, which, though effective, often encompassed large three-ring binders covering detailed policies and procedures and pre-written (holding) statements for multiple crisis scenarios. Today, plans generally are leaner and more functional. While the more lengthy plans cover a large landscape of concerns and include important policies and procedures, they often are too cumbersome for use in an actual crisis.

The large volumes are useful as policy references, but the most useful crisis plans are the briefest, easy-to-reference documents—in hard copy and online. These policy references can be especially useful for predictable situations some companies may face or have faced such as hurricanes, industrial accidents, etc.

Because the management and communications functions are closely linked, these issue areas are frequently useful when presented in the same plan.

While the plans discussed in this section are assumed to be at the headquarters level, it is important to "drill down" or require that each subsidiary develop its own subsidiary-specific plan and that, further,

each location have its own plan. It is assumed that the HQ model can serve as a guide for these "drilled down" plans.

Ownership of the crisis communications plan is important on two levels:

First, an effective plan is as good as its stewardship—and the best plans are owned by and kept alive by a designated senior staff member who has specific responsibilities for keeping the plan updated and current. All members of the crisis team charged with participating in the crisis plan should be held accountable. Their crisis responsibility should be part of their job descriptions and their performance should be included in annual reviews.

Second, the core elements—i.e., the functional responsibilities of each team member—are most useful when each team member has played an active role in writing that portion of the plan.

For example, a checklist for communications might include:

- Upon notification of a crisis, immediately notify key communications staff as follows: (list names)
- After initial briefing on situation, determine who will participate in immediate communications, and brief communications staff.
- Initiate media and Web monitoring.
- Begin initial press release drafts.
- Begin initial employee announcement draft.
- Initiate log of media calls.
- Determine response to media calls (if any).
- Determine need to schedule press conference.

- Designate an appropriate spokesperson and begin preparation.
- If press conference is scheduled, determine the following:
  - Location
  - Time
  - Notification
  - Opening statement
  - Anticipated Q&A
  - Rehearsal

The table of contents for a functional crisis plan should include:

- General/company-specific policy summary. Typically, this section will include reminders on safety priorities, corporate commitment, and policies concerning international and other locations.
- Crisis team roster—and alternates—with all contact numbers
- Support team roster—and alternate with contact numbers
- Security communications section—including functional checklist and CEO COM Link procedures
- Crisis communications room checklist
- Functional checklists for all crisis team and support team members
- Media procedures and reminders
- Risk communications guidelines

- Holding statements
- Key facts about the company
- Crisis prevention procedures
- Dark Website and other Web procedures

Holding Statements:

Many crisis plans include holding statements—essentially a series of "fill-in-the-blank" media statements for a number of predictable events such as hurricanes, fires, workplace injuries, etc. These can be useful documents which save time during an emergency or crisis; and which assure that all the right elements are included in a press statement. Caution: when adding holding statements to crisis plans, be certain to label the documents: *Holding Statement. This is not an Official Document.*

For unpredictable or potentially severe post-9/11 threats, holding statements present new challenges. It is useful to first consider a set of criteria against which statements should be judged when they are written during actual events. These criteria include:

- What happened—including a description of injuries or fatalities; harm to physical structures;
- Where the incident occurred;
- Cause if known—if not known, do not speculate;
- Next steps.

In all situations, it is essential that life and safety issues be given top priority, with appropriate expressions of concern.

The following is a template for a holding statement, which might be issued in the first hour after an attack or other disruption. It is intended only to provide some guidance on points that should be included in a holding statement.

SAMPLE HOLDING STATEMENT.
THIS IS NOT AN OFFICIAL DOCUMENT.

(city) (date) The (name of facility) or (name of company) this morning was struck by a series of explosions which shut down all electric power within a radius of approximately (number) miles covering the (name) metro area. Several fires are burning at the (name of facility) and all available fire and rescue facilities are on site working to control the fires.

Our first priority is the safety of our employees. At this time, there is no information on injuries or fatalities. On a normal workday, there are approximately (number) working at the facility.

Backup power generation for the (name) metro area is in the process of being switched through (name) system and initial plans are to have power for the area within the next three to five hours.

Additional reports will be provided to the media via email and on the Internet at a specially activated site (name of site).

Notes:

1. Create a Holding Statement

What happened:

When:

Where:

How:

Actions underway:

2. Create a Team Member Checklist

Staffing:

Actions:

Immediate Day One

Long-term Day Two

Day Three

Investigation or Fact-Finding Duties:

Communications:

To Customers:

To Staff:

To Government:

To Vendors:

Notes:

Establishing a Crisis Team Structure

There is no single element to managing a crisis that is more important than the people who make up your "crisis team." These are the professionals who are charged with making the decisions—and often times carrying out the tasks—that will impact a company's safety, reputation or operations. It is imperative that these individuals possess basic, but important characteristics such as decisiveness, patience and an eye for detail. While leadership is a crucial quality in a crisis, clearly it is counterproductive to have too many "chiefs."

Members of the crisis team should be defined in advance, and it is always wise to have alternates or a designated reserve for each in the event they are completely unavailable (possibly out of the country, out for medical reasons, a personal crisis, or other reasons). All team members and alternates should take part in company-specific, periodic training sessions and simulations. Participation in training should be mandatory and tracked so there is a record of those who are crisis-ready.

Likewise, when turnover occurs, it is especially important to provide all crisis materials and training to new team members and alternates. Always update contact information immediately.

CRISIS TEAM STRUCTURE

Within the crisis team structure, there are four key tiers that should be defined during the prevention and protection phases. These four tiers include the Senior Crisis Team, the Subsidiary or Plant Location Team, the HQ First Response or Screening Team, and the HQ Support Teams.

1. The HQ Senior Crisis Team

- President/CEO
- Senior executives in charge of the following areas:
  - Communications
  - Legal
  - Marketing
  - Security
  - Information technology
  - Operations/ Manufacturing
  - Human resources
  - Government relations
  - Public affairs
  - Financial
- Others may be added as needed, depending on the situation—e.g., supply chain/purchasing; specific facilities managers, etc.

  An alternate (or delegate) should be designated for all crisis team members. All relevant alternate contact information should be circulated. Alternates are utilized when primary team members are not available and when a crisis runs after hours—through the night or for days. Alternates can relieve primary members during stressful and exhausting days.

2. Subsidiary or Plant Location Team

It is important to recognize that the first essential personnel in the notification chain may be a facility manager, rather than someone at corporate headquarters. Communication between those "on-site" personnel and the corporate crisis team members is typically the crucial point in effectively managing the crisis.

Each subsidiary and site should develop and keep up to date a localized plan that accounts for:

- The nature of the operation
- Staffing
- Special vulnerabilities, including history of past crises
- Local variables in community, government or media characteristics

These plans should be modeled after the corporate structure and reviewed periodically with the senior HQ executive responsible for crisis communications.

3. HQ First Response or Screening Team

This is the team, generally consisting of a small group of three or four staff and headed by a duty officer, who receives first calls and works immediately to determine the nature of the situation and if indeed a crisis has occurred—or if it is a local emergency which can be corrected quickly. While this First Response or Screening Team is assembled on a case-specific basis, the team is generally drawn from:

- Communications
- Security
- Business contingency and disaster recovery managers

- Manufacturing/Operations
- Information Technology
- Building/Facility Management
- Human Resources
- Legal

Note that emerging crises, especially ones which may have connections to security, should at all times be reported to the full senior crisis team—regardless of status and including those in the fact-finding stage. This communications system can easily be accomplished by an email system.

4. HQ Support Teams

There are at least two types of Support Teams:

1. Crisis Support Team, which generally is assembled as needed once a crisis is underway, consists of those staff who are given assignments for investigations, fact-finding, on-site response (the "GO" Team), communications support, etc. as needed—and as directed by the senior team.
2. Crisis Room Support Team, which generally consists of two or more assistants for phones and other support work, is an important adjunct to the Senior Crisis Team and should be notified at the same time as the team to be available for all support in the crisis room

   Other support teams may be added as needed, including a communications team, community support team, etc.

FLEXIBILITY AND DECISION MAKING

Companies could encounter conflicts over lines of responsibility and decision-making authority during a severe crisis, which could pose an imminent threat to safety. At the same time, depending upon the event or threat, certain decisions may need to be made very quickly. Senior management may not always be a part of, or available to, the First Response Team, and team members can find themselves in a challenging scenario in which they have a unique responsibility to make decisions about company operations.

However, once the first steps have been taken to ensure safety, all further actions, such as speaking with the media, should be coordinated with senior management and/or the corporate HQ.

Here is a sampling of the decisions that may need to be made without the input of senior management as a result of an imminent threat or event:

- Facility work stoppage, evacuation or closure of a facility due to an imminent threat (those involved include the facility manager or head of manufacturing / operations)
- Notification of local authorities
- Response to local media regarding a rumor or possible threat (those involved include facility manager, communicator or designee)
- Communicating to facility employees regarding a possible imminent threat (those involved include facility manager, human resources or communicator)

Senior management can minimize the danger of mistakes by facility or non-senior crisis managers by clearly defining the criteria for making decisions in the immediate aftermath of an event, such as

when to evacuate a facility or when to respond to local media. While establishing these criteria is important, management must understand that designated crisis management or on-site management personnel may be uniquely empowered during a crisis. This underscores the need to seriously consider the makeup of crisis teams and the crisis readiness of those individuals who manage facilities.

Notes:

Crisis Team Contact List

	Name	Title	Office #	Home #	Cell #	Pager #	Weekend #
Primary:							
Alternate:							
Primary:							
Alternate:							
Primary:							
Alternate:							
Primary:							
Alternate:							
Primary:							
Alternate:							
Primary:							
Alternate:							
Primary:							
Alternate:							

Notes:

Using CEO COM Link and Other Communications Tools

A number of tested and reliable technological tools can be established and maintained for CEO communication in preparation for a crisis. Below are some examples of the best tools. For purposes of this section we have focused on recommendations regarding both levels of crisis that a CEO may have to help manage: a major national crisis such as 9/11, or a company-specific crisis in which the CEO is working with the company's crisis team. In either case, redundancy of systems is especially important, given the unpredictable nature of potential crises.

PART 1: ROLE OF CEO COM LINK

The Roundtable's CEO COM Link is a tool through which corporations can efficiently and effectively communicate in the event of a major national crisis. Should another event similar to 9/11 occur, CEO COM Link would provide a means for information sharing among companies, and between the companies and the Office of Homeland Security or other relevant government bodies. An important component of CEO COM Link is the notification system whereby CEOs would be alerted by multiple methods such as phone and email. This redundant notification system increases the likelihood that a CEO will

receive notification that a CEO COM Link call has been scheduled. BRT member CEOs must register and be credentialed before they can gain access to this crisis tool, and will receive separate instructions on using the system.

GETS Cards for a National Crisis:

The BRT has provided Government Emergency Telecommunications Service (GETS) cards to its CEOs. These cards provide priority telephone connectivity to parties considered by the federal government to have a role in addressing issues related to homeland security. The GETS cards will also enable CEOs to gain access in a crisis to potentially congested phone lines at the time of a CEO COM Link call.

PART 2: OTHER CEO COMMUNICATIONS TOOLS

CEO Notification in a Company Crisis:

Inevitably, there are times when a CEO may not be easily accessible through routine means in the event of a crisis. In these cases, companies may want to consider a CEO and crisis team notification system similar to that available under CEO COM Link. Multiple automated calls to the offices, homes and cellular phones of the CEO and crisis team members, in addition to an e-mail or fax, would give greater assurance that the CEO and crisis team can be quickly assembled.

Whoever is designated as the company's duty officer should be responsible for mobilizing the crisis team, including the CEO (see Crisis Team section).

CEO Communication to Employees:

Regardless of the decision as to who is the most appropriate spokesperson for the company (see Spokesperson / Leadership Communication section), countless case studies have shown that employees expect to hear quickly from the company's CEO when a crisis has struck. Communicating the CEO's concern about the safety and well-being of the company's workers can be executed internally through a number of methods and should be done as soon as possible during and after an event.

The tools that are used to link a CEO to the company's employees are as varied as the methods used to communicate with employees in a normal working environment. Furthermore, those methods that a company normally uses to reach its workers are the best channels to reach employees during a crisis. A backup system should also be in place in the event normal channels are not operating or employees are unable to report to work. In the latter case, local radio and TV provide an important means of communication.

The level of attention devoted to a company Intranet and email system increases during a company crisis—even among employees who do not typically access either tool. Therefore, an email update from the CEO or a Web-based audio or video update from the CEO may be appropriate. Web-based audio and video can be done much more quickly and much more cheaply than one might expect (see Developing Web-Based Communications for more about Intranet and email communication).

PART 3: CRISIS NOTIFICATION SYSTEM

The way in which a company is organized to receive a first call and to implement its response is a critical factor in the crisis equation. While some crises may be apparent—such as a terrorist attack—others may be less obvious and need to be checked quickly to determine the severity of the problem and whether it constitutes a crisis.

Informing and Contacting

First, it is important that senior management is not sheltered from early warnings. A company should develop a system for keeping senior management informed daily—in succinct form—of potential problems.

Priority #1:

Essential phone numbers—for the crisis team, alternates and key outside sources, such as vendors, customers and local law enforcement—should be easily accessible and up-to-date at all times.

Although pocket/wallet cards have generally been regarded as a convenient format, the recent proliferation of contact numbers (cell phones, pagers, etc.) for each person, plus the names and numbers for alternates, precludes the use of small wallet cards. A slightly larger format, with an accordion-shaped card in a small, durable slip case holds far more information and can conveniently be stored in a briefcase, glove compartment, home nightstand, etc. (See back jacket of Toolkit.) For those using a personal electronic organizer, such as a Palm Pilot or Blackberry, this information can and should also be stored electronically; and online in a secure site. (Note: Wallet-card size CDs can hold many phone numbers and play in any computer CD reader.)

Priority #2:

A second list of contacts, such as customers, vendors and community resources should be up to date and readily available. This list obviously is more extensive and cannot fit onto small formats. For this purpose, an online site backed up by hard copy should be maintained and accessible to the team.

First Response

First calls should all go to a duty officer, who is part of the senior crisis team. In general, all crisis team members, including communications senior staff, should serve on this roster. This duty officer (or an alternate) can serve on a schedule, which rotates weekly. The schedule should be circulated among the crisis team members and security. Together, the duty officer and the security officer should develop a procedure to verify the authenticity of the caller.

A first call may come in to a variety of sources at any time—and all key points of entry for these calls should refer the calls to the crisis duty officer or alternate immediately. The duty officer will then determine whether or not to activate the entire senior crisis team, one or more members, or to refer the problem to a screening or fact-finding committee first. Some general guidelines for determining first steps can be addressed through a series of questions:

1. Is there an immediate threat to safety?
2. Is the source of the threat a credible one?
3. Have there been any fatalities?
4. Are the media calling?
5. Has this been reported in the media?

6. What is the threat to my facility?
7. Have any facilities been damaged, threatened or destroyed?

Activating the Crisis Team

Once a decision has been made to activate the crisis team, time is a critical factor. Although some duty officers may prefer to make their own notification calls, the number of calls needed to reach individuals, especially during off-hours, becomes time consuming. For that reason, some version of a "telephone tree" can be an effective approach for activating the team. In structuring a "tree"—i.e., a simple sharing of calls, consider two approaches:

1. Each security staff member calls two or three team members, who in turn will call other team members. All calls should be scripted.
2. Duty officer directly calls two or three team members, who in turn will call other team members.

While the "tree" concept is theoretically workable, it may not be practical or safe for a team member who is driving during a crisis, for example, to make calls. Trees generally work best during normal business hours when calls can be made by team members at their desks. When it appears that the tree system is becoming too complicated and burdensome, the duty officer should assume responsibility for all calls.

Test the Notification System Regularly

Once each quarter, the notification system should be tested to determine that all members of the crisis teams and their alternates can be contacted. This should be conducted at various times—i.e.,

during office hours, weekends, and evenings. Each call should be simple and brief—such as:

> "This is a test of the XYZ crisis team system. Is X at home (in the office)? May I speak with him/her, please?" Then thank the individual for responding. "This has been a test and we appreciate your response. No further action is needed."

If the individual is not reached, messages should be left at all contact numbers asking for the individual to call in for information.

Notes:

Notification Test Log

Team Member	Numbers Called	Time	Success	Failure	Notes

Notes:

Establishing Spokesperson / Leadership Communications

A great deal of attention has been placed on the role of the spokesperson in recent years, and while examples abound, none stands out more vividly in light of 9/11 than that of Rudy Giuliani. It is generally agreed that he bypassed all partisan politics not only as a spokesperson delivering sound bites and interviews, but also through his presence among those who were suffering and who needed encouragement and thanks. Words were important—but equally important were the visual images of his movement around the city.

While it is difficult to predict the nature of another attack—and whether or not the demands of a spokesperson would be the same—it is useful to examine the characteristics of a spokesperson under pressure.

The best spokesperson:

- Has a senior title.
- Has extensive knowledge of the company, and the situation (or can access it).
- Has the self-discipline to stay "on message."
- Is continuously updated on the situation.

- Has high energy and is able to sustain that energy under pressure and possibly multiple interviews.
- Is able to remain calm.

Seniority is especially important when:

- Widespread public health or safety is concerned.
- Injuries and fatalities have occurred.
- National or international media are covering the crisis as major news.
- The Office of Homeland Security and other government agency heads or cabinet level officials are communicating to the public on the same or similar topics.

While virtually every crisis plan contains concise communications tips for spokespersons, the following is a good summary:

- **Develop 2-3 key messages at most—**thus maximizing the chances that the audience will grasp your messages.
- **Know your objective,** and personalize your messages for the audience. Make your communications objective as clear, simple and as memorable as they can be. What is the purpose of the interview? What do you want readers/viewers/listeners to take away?
- **Be honest, frank and open.** When communicating risk information, trust and credibility are the most precious assets.
- **Speak clearly and with compassion.** Technical language and jargon are useful as professional shorthand, but are barriers to successful public communication.

- **Use anecdotes or examples.** Support your key messages with anecdotes, examples, comparisons, etc. These will lend credibility to your answers, help to "drive home" your messages, and bring the interview to life.
- **Be succinct.** Keep each answer to a few lines. This is especially important for TV and radio, which deal with sound bites. Newspaper and magazine quotes likewise are often brief—a few sentences at most.
- **Anticipate the tough questions.**
- **Know what you want to say and don't want to say.** Don't be afraid to repeat your key messages. When possible, state your conclusion first. Then reinforce it with a few supporting statements or examples.
- **There's no such thing as "Off the Record."** If you don't want to be quoted, don't say it!
- **Don't speculate.** Beware of hypothetical statements, and stick to your agenda.
- **Make eye contact.** Talk to reporters—not cameras.
- **Speak with one voice.** Make sure you and other company spokespersons are delivering consistent messages.
- **If the reporter asks questions you can't answer,** it's OK to say, "I don't know." Just make sure someone who can answer the question gets back to the reporter in time for his/her deadline.

Notes:

The following persons should be considered for a spokesperson role:

What type of training is appropriate?

Has spokesperson training occurred?

Is retraining required?

Notes:

Understanding Risk Communications

"I didn't want people surprised by things that would then frighten them more. It has always seemed to me that the best way to do that is to share with people as much information as you can, and explain it in the clearest way you can explain it. Almost anything you understand is less fearful than something you don't understand. No matter what danger, what risk you face, if you can understand the risk, then you can understand the danger. And the more you understand about it, the more you take the irrational fear out of it."

Rudy Giuliani, Former Mayor of New York City
Interview, *Catalyst Magazine*, March 2002

Fears and uncertainty are synonymous with the uncontrollable results of an attack. And employees, customers and the public need information and reassurance, not probability statistics, odd comparisons or jargon. In fearful circumstances, the toughest demands are made on spokespersons. The Best Practices that follow are based on multiple research efforts and testing, and are especially relevant in times of widespread concern.

Risk Communication research has shown that:

- People more readily accept risks when they can control the situation, such as driving a car or choosing to participate in high-risk recreational activities.
- Situations in which people have little or no control—i.e., a terrorist incident—present major risk communications challenges in order to overcome fears, dispel rumors and provide survival information.

The Risk Communications guidelines that are most effective include:

- **Being honest and clear.**
- **Respecting the public's concerns and intelligence.** Recognize that the public is savvy and will reject and be angered by any communication which is superficial or patronizing.
- **Telling the facts,** admitting the unknown and committing to a continuous flow of information as it becomes available.
- **Acknowledging the crisis at the earliest stages.** Even when the facts or implications are not known, it is comforting to know that leadership—who will be expected to be seeking solutions—is aware of the event or crisis.
- **Quoting credible and other trusted sources—**such as university-affiliated scientists or senior officials at government agencies.
- **Showing empathy and compassion to those affected by the crisis.**

In communicating risk, companies should avoid:

- Jargon, such as "parts per million." The public simply has no idea what a "part" is. If possible, make a comparison to something simple. If not, do not make the comparison.
- False or overly optimistic statements of assurance.
- Presumptuous statements like, "I know how you feel" which is often met with the reply, "No you don't."
- Unreasonable comparisons and extreme statistics. A "one in a million chance" may seem minimal—but think of the individual who fears he or she may be that one.
- Statements such as, "It's safe enough for my family and me." The fears which may present are simply too deep and complex to be dismissed with such simplistic endorsements.

Notes:

List company-specific risks.

For each risk identified above, consider points to be made in a risk communications statement.

Notes:

Controlling Rumors

Rumors may become a substitute for facts during a crisis. The sooner rumors are dismissed and corrected, the more likely the public can be reassured and protected - and panic avoided.

Rumors can be effectively controlled or refuted by:

- Assigning a member of the crisis team (e.g., a designate of the senior communications team) to monitor media and other sources for rumors and rapidly refute them through the appropriate, targeted media—in most cases through the same media the rumors were disseminated through.
- Using facts and statements stating, "We do not know" when appropriate.
- Quoting recognized authorities.
- Avoiding lengthy repetition of negative statements or the rumor itself.
- Employing multiple communications techniques to disseminate accurate information, including:
  - The Internet/Intranet
  - Email to media
  - Email to employees
  - 800 number and other numbers to call for information
  - Electronic as well as "old fashioned" paper message boards

Notes:

Notes:

Establishing and Maintaining a Crisis Room

The Crisis Communications Room, or "War Room," is generally the nerve center for crisis communications and the entire crisis management team. It may be supplemented (depending on the specific crisis) by a local "war room" at the actual site of the crisis, by emergency command or infrastructure centers, or other rooms that support the management of the crisis (such as an emergency call center for public or customer questions; or a medical support team if there have been accidents).

The ideal Crisis Room is:

- Easily accessible and secure
- Able to be activated within less than 10 minutes
- Fully equipped with state of the art communications facilities
- Able to comfortably and functionally accommodate the Crisis Team, with adjacent spaces also available for breakout meetings, if needed

Should the Crisis Room for any reason be inaccessible (power failure, physical damage, etc.) an alternate location should be pre-designated. This could be at another location at HQ or at a nearby hotel or other facility distant from HQ.

The room and all of its equipment should be configured so that they can become fully operational at any time 24/7. This requires more than simple access—provisions should be in place to supply ventilation, power and computer network access at any time.

Consider the following:

- Most War Rooms are used as regular conference rooms in order to maximize the cost efficiency of the space. Because a crisis could occur at any time and because the primary purpose of the room is for crisis purposes, all staff reserving the room for non-crisis purposes should understand they could be preempted at any time on very short notice.
- If the room is to be used for regular meeting purposes, all crisis-related equipment (phones, display walls, other equipment) should be secured in locked cabinets. All of this equipment should be quickly accessible, put in place and activated within 10 minutes.

  The general parameters for the equipment:

  - Separate phone extension and instrument for each seat at the table
  - Laptop port at each seat
  - Multi-directional speakerphone at center of the table
  - Electronic display wall which may include facilities for video playback or broadcast monitoring; maps; crisis log; PowerPoint; technical diagrams; videoconferencing; etc.
  - Fax machine
  - Copier
  - Printer

  - Easels with flip charts; or chalk board with print capability

- Room should be staffed with at least two or more support personnel to handle phone calls, copying and fax and IT support.
- A detailed maintenance and activation protocol should be established along the following guidelines:
  - Establish responsibility for activation. Generally this is a responsibility of facilities management personnel.
  - Schedule a monthly walk-through of the room to be certain that all facilities are intact and operable.

Notes:

Crisis Room—Maintenance Checklist

Item	Availability?	Properly Working?

Notes:

Developing Web-Based Communications

The ability to quickly collect, analyze and disseminate information in times of crisis is absolutely critical. In today's world, this can best be done through a clear understanding and utilization of Web-based technology combined with traditional tools, such as telephones and pagers. Tested and reliable technological tools should be used, but questionable, untested "tech toys" should be avoided. In a crisis, organizations may collapse around unreliable technologies that they have instituted simply because they are seen as "cutting edge."

While many companies do not have Web-based technologies readily available to all of their employees, it is the fastest growing communications medium and it is only a matter of time before it permeates into the daily life of every American, and, eventually, every global worker. Here, we will focus on Web-based technologies, though these are in no way intended to replace diversified reliance on traditional communications tools such as telephones, faxes, radio and television.

PREVENTION AND PROTECTION

The Internet:

The Internet is a very useful tool in both crisis prevention and protection. By making it a top priority to monitor any Internet activity relevant to your company (this should also include other Web-based

technologies such as chat rooms, newsgroups and e-mail campaigns), a company can increase the chances that it will identify early warnings of potential sources of a threat, whether they are competitors, activists, former or current disgruntled employees, consumers or any one of countless other catalysts for a crisis.

Clearly, once a company is aware of any emerging threats it may be able to utilize its Website, in coordination with other methods of external communication, to disseminate a response to the potential threat.

For example, if a company has identified a potential threat to its reputation arising from an impending attack from activists about a particular environmental issue, it may be able to help diffuse consumer concern and activist interest by communicating its position and proactive approach to the issue via its company Website. Because criminals—and now clearly terrorists—often use the Internet to gather intelligence for an attack, a company may also choose to utilize its Website as a place to publicly convey the priority that the company places on its safety and security. If a threatening body sees this, it could help to reduce the chances that the company will be a target.

Intranet & Internal Email:

The company Intranet can be a valuable tool in conveying to employees a company's procedures for crisis-related events such as evacuations or other types of business interruptions. All policies and procedures for crisis events should be clearly outlined in a page accessible from a company's Intranet homepage and should be carefully written following the guidelines of effective risk communication. A company-wide email should be sent out on a quarterly basis to remind employees to review safety and security

procedures in the event of a crisis. Also, the specific procedures applicable to a particular event should immediately be emailed company-wide and prominently highlighted on the homepage.

E-training:

Another valuable tool is online E-training for crisis preparedness. There are a number of Web-based products that offer a full integration of audio and video with PowerPoint presentations, document links, email feedback mechanisms, live chat and even crisis simulations or tests, all on a secure Intranet site. These can be prepared for "on demand" training in which employees are given a set period of time (often 30 days) to access the site, follow the audio/video/PowerPoint training and respond to the simulation scenario, test, or simply provide feedback through the email feature. The training can also be done using live audio and video, but the cost is generally significantly higher and the "on demand" convenience is obviously lost. All feedback information can be collected into a database for monitoring and analysis by management.

RAPID RESPONSE

Intranet/Crisis Management Site:

Increasingly, the public is turning to the Internet for breaking news and information. This is also true of employees and an Intranet when a company faces a challenging situation. Research shows that many employees who might not normally access the company Intranet will find a way to do so in a crisis situation.

A crisis management site can be developed for housing your crisis plan. This site should reside on a highly secure server and should require a password in order for crisis team members to log on.

Crisis management sites will generally include information such as 24-hour contact information for all team members, address lists for business unit managers, crisis procedures, checklists, etc. This is essentially the "virtual" and "interactive" version of your crisis plan. Some organizations have attempted to make the crisis management site fully interactive with fields to be filled in, which walk the crisis manager through several criteria in order to help direct them through the process. While this has been highly successful in some cases, it can become burdensome and impede the flexibility that is necessary when every second counts. Above all, keep your crisis management Intranet site simple, just like your crisis management plan. Checklists, procedures and important contact information should be housed there, and little else.

Dark Websites:

Dark Websites are a tool that can be used effectively for both internal and external communication. For disseminating information to the public and the media, a dark Internet site, designed and constructed well in advance of an event, can help a company reach its external audiences very quickly. Whether your company is hoping to communicate to the media, consumers, investors or all external audiences, a template Web page should be constructed for each audience, with an overarching "crisis" dark homepage prepared to serve as a gateway. There will be information specific to an event that clearly cannot be included in advance, but the framework for the crisis site can be prepared. This will allow your company—at the time of an event—to not be burdened by all of the questions you might otherwise ask such as "Who needs to have links on the site?" or "What materials need to be accessible from the site?"

As discussed earlier, press materials and public statements can also be pre-designed for a number of different scenarios. Again, specifics to the event will have to be plugged in, but the basic work can be done in advance, thereby reducing the time that it will take your company to communicate with your audiences. Your company's Internet homepage could quickly and easily be linked to the crisis Website where all information could be made available to your external audiences.

In many cases, a company may find it useful to communicate event developments internally before communicating them to the public or the media. Various dark Websites for use with the company Intranet can be prepared and often launched before any external communications are delivered.

Another use for a dark Website—both internally and externally—is the use of Web-based audio and video to communicate directly from the company's CEO or spokesperson. A dark Website can reserve a portion of the site specifically for the broadcast of a message from the company CEO or spokesperson, and with surprisingly affordable software and very simple video technology, a message can be recorded and uploaded to an Internet or Intranet site in less than an hour. Few companies have the access or resources to do this through satellite video or other traditional mediums in such a short period of time.

Web-based technology can also be easily set up for a one-way live broadcast, but most organizations are not yet sufficiently prepared to use real time two-way Web casts as a means of communication internally or externally. The traditional telephone conference call is still the most effective and efficient method for reciprocal communication in response to a crisis.

Email as a notification tool

Email is a valuable means of notifying employees or external audiences of the posting of important safety information, the launching of dark Websites or immediate developments relevant to an event. You can drive traffic to your crisis sites by distributing a notice via email.

An external email address book can be set up in advance with the email addresses of reporters, important customers, vendors, etc. A company can add to this list throughout the management of the crisis as well. This will enable outsiders to input their email addresses in order to receive updates whenever there are new developments to communicate. Be sure that your external dark Websites contain a registration field or input point for visitors to register their email addresses in order to receive immediate notification of updates.

Crisis Monitoring:

During a crisis, one of the most important Web-based elements must be the monitoring of Internet information related to a company. Just as it is unwise to not seriously consider all threats identified on the Internet in advance of a crisis, it is crucial to not overlook the communications being shared on the Internet during a crisis. If possible, a company should have a person dedicated to monitoring on-line activities on sites that focus on the industry, including sites for trade associations, activist organizations and competitors—just as companies monitor the Web for media activity.

Technology Reliability/Backup:

During a crisis, concerns often surface regarding the reliability of an Internet server and the accessibility of a Website. To avoid these issues, a company should identify a secondary server where it will

maintain duplicates of the dark Websites that it has prepared. Most organizations have offsite data "warehouses" or "virtual safety deposit boxes" where their important information is duplicated and secured. It is recommended that all crisis data be housed in these backup servers as well, in case the primary server is damaged or destroyed in an event.

A company should also be prepared for very high levels of traffic to any sites designed to be used during a crisis. Therefore, there should be substantial server space reserved for a crisis and that space should be dedicated to the crisis sites during an event. Going to a lot of trouble to design and launch crisis sites that are ultimately not accessible because of a lack of server space is an obvious waste of resources. In some cases, a crisis site replaces an organization's normal site altogether. While this generally provides sufficient server space, it is advisable to have additional reserved server space or the ability to link to another server in a time of crisis.

It is up to senior management to convey to information technology staff the priority that is being placed on crisis management to ensure that the company is prepared to use these sorts of Web-based tools in the event of a crisis.

Notes:

Review your Web capabilities to determine how they can be enhanced.

Notes:

Preventing a Crisis

"As a country, we must come to understand the enduring vulnerability of a free and open country, an enduring vulnerability to the possibility of terrorist threat and terrorist attack. We must also understand that individuals, organizations, companies and communities all have a new role in helping to provide for homeland security."

Governor Tom Ridge, Director of the Office of Homeland Security
April 8, 2002

Communications play an especially important role in spotting early warnings, which may affect one company, an industry or the nation. Clearly, the best crisis is one that never happens—and this is especially relevant to security.

Companies should establish open communication lines to all employees, customers and vendors to give 24/7 opportunities to come forward with suspicions, concerns and suggestions aimed at crisis prevention. Do not assume any early warning is too small or insignificant to check out. And the simplest, most direct method is often the most productive.

All communications methods should be:

- Easy to use and free of bureaucracy or what could be perceived as intimidation. For example, a hotline or email suggestion box housed at the general counsel's office could be perceived as intimidating and thus it could discourage communication.

- Structured so that all messages are quickly checked out—and responses given to the person submitting the message.
- Fully explained so that everyone understands how information is reviewed.
- Kept fresh—i.e. suggestion boxes should be kept in their same positions; posters updated and replaced periodically, etc.
- Sensitive to employees who are reluctant to come forth with ideas or problems. One simple approach is to regularly report—without names—the suggestions and responses in the employee newsletter.

Any executive charged with reacting to and evaluating suggestions and early warnings should be briefed/trained on the system and given specific, consistent guidelines to follow.

Feedback or suggestion tools to include in a prevention program could include:

- 24/7 telephone hotline
- Paper suggestion boxes
- Regular employee focus groups—as separate from consumer or external focus groups. Companies can provide preparatory materials to employees in advance to stimulate thinking.
- Email hotline
- Reminders in newsletters and on posters in high circulation areas
- Employee surveys

When a specific lead has prevented a crisis, the individual(s) who provided the lead should be recognized and rewarded, unless they chose to remain anonymous. A reward can take many forms—from a day off to monetary or stock rewards.

The Question of Anonymity

Though employees may have concerns about identifying themselves, they should understand that early warnings are very serious matters and rely on every detail, including the need to know their identity. But while it may be very useful for leadership to know the source of the early warning, in most cases, there may be no need to publicize it. In the case of information received through employee focus groups, discussions and sources are always held in confidence with no disclosure of names, though employees know each other.

Notes:

Employee Communication Worksheet

Inventory of Program:	Current	Future
Electronic email	_____	_____
Pager/suggestion boxes	_____	_____
Phone/hotline	_____	_____
Focus groups	_____	_____
Staff meetings	_____	_____
Posters	_____	_____
Other	_____	_____

Over the past six months, how many suggestions (of any nature) were received? _____

How many were answered? _____

How many yielded solutions to problems? _____

How many averted a crisis or prevented a small problem from becoming larger? _____

Did employees receive answers privately? Publicly? _____

Were employees rewarded? _____

Sample Poster Concept

Implementing Crisis Training Techniques and Simulations

Training sessions, generally designed and conducted by outside consultants and combined with simulations, are the most effective way to:

- Keep the crisis team up-to-date on their skills.
- Identify, through post-session debriefings, vulnerabilities, which, if corrected, can avoid crises.

Training sessions for crisis teams are valuable though they should be kept as brief as possible allowing for discussion and some level of practice or simulation. Typical effective training sessions run two hours and include:

- Review of company plan.
- Debrief on latest crises or near-crises.
- Discussion of prominent crises in the news and lessons learned.

Several formats for simulations are effective, depending on the proficiency of the team and the needs of the moment. The formats are:

1. **Tabletop or discussion.** The advantage of this format, which is conducted in a conference setting, is that it is the most informal and is structured around one or more

scenarios being posed to the team—who is asked to provide its action plans for its respective responsibilities. This is generally useful as a refresher for highly experienced teams to discuss new vulnerabilities. *Average duration: two hours.*

2. **Mock press conference.** This format, which is growing in popularity, consists of a mock press conference based on a scenario posed to the team following a general training or discussion session.

   When the team is given the scenario, they are told they have 30-40 minutes to discuss their strategy for solutions and their key communications messages. They are free to designate whomever they believe is appropriate as the spokesperson. Once organized, the mock press conference commences, with the trainers and any of the team members who wish to participate by playing the role of reporters. The press conference is recorded on video and then played back for critique. When time permits, a second round is conducted, with either an escalation of the original scenario or a new scenario. This is a generally useful format for companies with newly revised plans, and for companies which have little experience with crises. *Average duration: two hours.*

3. **Simulation.** This format is a full test for the team and any support they may call upon within the organization. It begins with a phone call to the duty officer, in which an employee, reporter, government official or other source announces a problem. The problem is always of the level at which the team would assemble immediately in the war room. Using a set of "rules of engagement," the team, which has been

called by the duty officer, then begins to work together as if the problem were actually occurring. Pressure mounts and the scenario develops as a series of scripted phone calls flow continuously to the war room, asking questions, announcing new developments, etc.

The team is allowed to call upon any resources in the company, with the strict proviso that every call, fax or email is prefaced by, and ends with, the phrase: THIS IS A DRILL. This format is generally advised for companies which may have experienced several crises. *Average duration: four hours.*

4. **War game.** This format is designed to test multiple locations and organizations. Large groups of employees and others generally are staged at actual locations and move about as if the actual crisis were taking place. It is the most ambitious format and because of the extensive, often open locations, it is subject to media coverage. This is a major commitment and is recommended as a test of multiple locations, bearing in mind it will undergo scrutiny by the media. *Average duration: 24-48 hours.*

Overall, preparation is key, as is the goal to present the team with the most realistic, highly vulnerable scenario possible. For this purpose, it is important that only one person within the organization know of the scenario in advance. This person is known as the "trusted agent" who, working with the outside consultants conducting the simulation, assures the most effective, challenging scenario.

Notes:

Consider the pros and cons of applying each type of simulation to your company. Which simulation works best?

Tabletop or Discussion

Mock Press Conference

Simulation

War Game

Keeping Your Company Crisis-Ready

The effectiveness of a crisis plan is in direct proportion to the way it is maintained. This requires putting the crisis function on the front burner, not the back burner—"I'll get to it when or if I can." The benefits are obvious and substantial, when one considers the momentum lost when a company is not ready to face a crisis; or when poor communication misses an early warning and a crisis, which might have been averted, actually occurs.

Consider the following responsibilities for maintenance and continuous improvement, coordinated by a full-time crisis prevention and preparation executive:

- Review and incorporate Best Practices on an ongoing basis.
- Conduct a semi-annual crisis simulation within the company—which, to be most effective, should be unannounced, based on a plausible though severe vulnerability, and mandatory for participants.
- Keep the war room ready.
- Keep all contact information current—and conduct a quarterly test to verify accuracy.
- Review prevention/early warnings procedures and reports.

- Review, through media, major crises occurring at other companies or industries, looking at lessons learned: Can this happen here? How would we have handled—or prevented—the same crisis?
- Keep the primary spokesperson (CEO) and backup ready for media response by periodically scheduling them for coaching and review sessions.

Notes: