Understanding Crisis Management

Risk assessment & planning are key to effective response

By Steven E. NyBlom

CRISIS MANAGEMENT PLANNING has received considerable attention over the past 18 months due to terrorist activities. Many companies are rushing to better address this much like they did during the months and year preceeding Jan. 1, 2000, in response to concerns over potential computer failures. Many SH&E professionals are being asked to lead these efforts, while others are expected to work closely with security, human resources and allied professionals to help develop plans.

Crisis management is a comprehensive subject that encompasses all aspects of business, including operations, marketing and media relations, distribution and legal matters. As such, extensive interpersonal communication is needed among the affected groups. Often, however, program components are developed in a piecemeal manner by the individual groups responsible for them, without the appropriate planning and higher-level oversight needed to ensure a cohesive, comprehensive program. As a result, in the author's opinion, many of the most-significant business concerns are not addressed.

Over the past 18 months, it has been said many times that crisis management planning is more urgent now than ever. This is not true; it should have been urgent earlier. The risks have been known for some time—the difference is that public perception has been heightened.

Steven E. NyBlom, CSP, CPEA, ARM, ALCM, *is assistant director, casualty risk control, technical services, with Aon Risk Services of Southern California Inc. in Los Angeles. In this position, he provides casualty risk control services to clients in manufacturing, construction, entertainment and recreational industries. He holds degrees in aeronautical engineering and mechanical engineering from the University of California, Davis. NyBlom is a professional member of ASSE, President of its Valley Coastal Chapter and Assistant Administrator of the Society's Risk Management/Insurance Practice Specialty.*

ASSE Crisis Management Survey

In February 2002, an online survey of some 2,000 members of ASSE's Risk Management/Insurance Practice Specialty (registered with the Society's Online Community) was conducted to determine these members' perceptions of their companies' crisis management plans, their involvement in the planning process and the impact of current events. There were 296 responses; while this does not represent a statistically valid sample, it offers a glimpse of ASSE member opinions. Since the respondents were ASSE members, it is reasonable to assume that they were safety professionals. Those with different areas of responsibility and experience—such as security, human resources and allied professions—would likely respond differently to many of the questions.

Questions and percentage answers are provided on pg. 24. Respondents represented a cross-section of industries, company sizes and number of locations covered by the plan. A wide variety of crises that had occurred in the 12 months prior to the survey were identified. Some 90.5 percent indicated that their company had a written crisis management plan, but less than one-third had had reason to implement that plan in the 12 months prior to the survey.

The plans are called a variety of names, including emergency response plan (62.8 percent), crisis management plan (18.9 percent), business continuity plan (6.1 percent), disaster plan (4.7 percent) and other (7.4 percent). This diversity illustrates the need to establish definitions and the scope of the plans in place. It also suggests that confusion may exist when discussing plans because those involved may not be talking about the same subject matter.

According to most respondents, their companies' plans had been updated during the past year (55.1 percent in the past six months plus 25.3 percent in the past 12 months). Most organizations (65.2 percent) had conducted mock crisis drills within that period as well. Although the survey shows that considerable effort has been directed at crisis management planning, some results demonstrate that many organizations are not as prepared as they should be. Disturbing findings include:

•35.5 percent have not implemented all crisis management plans.

•32.1 percent have not provided training to all crisis management team members.

•38.2 percent have not provided media training for key team members.

•37.8 percent have not addressed post-crisis counseling.

•33.8 percent have not established preferred vendors to respond following a crisis event.

Based on these results, it is clear that plans exist within many organizations and that safety professionals are significantly involved in the process (87.2 percent of survey respondents indicated that the SH&E manager is directly involved in the planning process). However, a significant number of respondents reported that these plans are often not well-implemented or are missing key elements.

Defining Crisis & Crisis Management

The most critical question to start the process is "What constitutes a crisis?" The answer will determine the nature and scope of a crisis management plan. A crisis has been defined as follows:

Crisis: Any incident that can focus negative attention on a company and have an adverse effect on its overall financial condition, its relationships with its audiences or its reputation in the marketplace (Reid).

Crisis management: Crisis management involves planning, organizing, leading, and controlling assets and activities in the critical period immediately before, during and after an actual or impending catastrophe to reduce the loss of resources essential to the organization's eventual full recovery (IIA).

A wide range of terms are used when discussing crisis management; these include business continuity and business recovery (plans designed to keep a business functioning after a crisis); consequence emergency planning (the planning phase to prepare for and establish plans for responding to disasters); disaster or emergency response (response to an actual disaster); and emergency preparedness.

Depending on one's background (e.g., risk management, safety management, government), these terms may mean different things. Each term has its place within the subject of crisis management. For example, some organizations define business continuity planning (BCP) as the whole process, with emergency response planning, crisis management planning and business resumption included under the BCP umbrella. Some of these terms are used to define portions of an overall crisis management plan, while others are used in a generic manner to mean the whole subject. In this context, "crisis management planning" refers to the issues from risk identification and assessment through the recovery and lessons-learned phases.

The Goal of Crisis Management Planning

The goal of a crisis management plan is for the company to survive the crisis with its reputation and assets intact. This may seem a rather simple and obvious goal. However, experience shows that many organizations do not address the planning process adequately enough to prepare for response. The importance of proper planning is demonstrated after a crisis has occurred. Many organizations fail following a significant crisis due to poor planning; others survive because of their plans and their response. For example, Johnson & Johnson had a significant crisis (drug-tampering scare) in the early 1980s. Bob Daretta, J&J's chief financial officer, said, "Frankly, your reputation is the most important asset you own" (Cox and Hawthorne). He made this comment after the firm spent $117 million to recall, test and destroy existing stock. Through its handling of this crisis, J&J was able to retain good standing with the media and the public.

The most critical question to start the process is "What constitutes a crisis?" The answer will determine the nature and scope of a crisis management plan.

The Crisis Management Planning Process

The separate phases of crisis management planning are addressed separately. They are:

•risk identification;
•risk assessment;
•crisis planning and preparation;
•mobilization and response;
•recovery;
•plan testing (IIA).

Before the planning process begins, however, overall responsibility for the plan should be assigned to an individual who will be the point person for the entire project. This person will act as a facilitator in bringing people together and addressing issues in a systematic manner. Given the importance of the subject and the need to involve personnel from all levels of an organization, the responsible individual must have the appropriate authority to ensure success.

Risk Identification

The risk identification phase is critical, as only identified risks can be addressed. This requires a broad-based team that represents all aspects of the company; it may include senior management, human resources, risk management, SH&E, security, operations, logistics, finance, information technology/services, facilities and legal. Outside resources, such as insurance brokers, insurance carrier safety professionals, specialized consultants, public agencies and community groups may also be of assistance.

The risk identification phase should include a detailed review of business operations and processes, suppliers and customers, product lifecycles, technology systems, public perception and company reputation, market position and human capital. All critical business functions must be identified. Each organization should also hold a brainstorming session with a wide range of personnel in order to identify any issues that might have been overlooked during the initial review.

The list of potential risks to which any given organization may be exposed is tremendous. Common risks include arson, bomb threats, civil protest, computer virus, damaged public relations, death of a founder or key manager, earthquake, employment practices, environmental incidents/pollution, extortion, fire, flood, hail, HazMat spill, industrial espionage, kidnapping, lost market share, mold, power/utility failure, product defect, product recall, product tampering, riot, supplier outage, technological breakdown, terrorism, tornado, union strike, war and workplace violence (NSC; FEMA; IIA; ACC). Economic risks, such as currency fluctuations, inflation, stock market declines and recessions, can also present crises. Situations involving natural forces and actions of people are of greatest concern to SH&E professionals.

Risk Assessment

The risk assessment phase entails categorizing or quantifying identified risks using a matrix that ranks them by probability of causing a disruption and the likely severity should something occur. Figure 1 presents a sample matrix. The matrix may also be expanded to identify relative cost to control the risk. For example, the likelihood of a company deciding to respond to a high-severity/low-frequency/high-cost-to-control risk is smaller than for a high-severity/low-frequency/low-cost-to-control risk. Once risks are placed on a matrix, a business decision can be made regarding which risks to address through controls and financing options and which to acknowledge but not address.

The initial risk assessment should include an evaluation of existing control or mitigation measures. For example, a building with a properly designed and maintained sprinkler system might be placed in the "moderate severity" category as compared to a similar building with no sprinkler system, which could be placed in the "high severity" category. Unfortunately, in many cases, proper control measures may not be in place. "Surveys by professional safety specialists indicate that many of the most basic control measures are not regularly used until serious injuries or fatalities have occurred" (Grimaldi and Simonds 561). [Additional information on risk matrixes and risk assessment can be found in ANSI B11.TR3 (2000); MIL-STD 882D (2000); Main; and Boytor.]

Interdependencies among business units and process bottlenecks should be closely evaluated, with functions that have wide-reaching impact given top priority. For example, if all products pass through one piece of equipment during manufacturing, then damage to that equipment would shut down the process (high potential severity). Just-in-time manufacturing and delivery models have resulted in lower amounts of on-site storage/warehousing; this has created a stronger dependence on timely arrival of products or

Communicating in a Crisis

By Janine Reid

Protecting company reputation and credibility during a crisis is the company's responsibility, one that must be taken seriously and addressed at the onset of the crisis. Failing to communicate the company's story or how the company is responding will cause the public to believe what they learn from the media—and competitors. Open, honest communications executed quickly and consistently throughout a crisis can maintain—and perhaps enhance—a firm's reputation.

•**Identify the company's audiences.** This refers to anyone who can have an effect on a business or its reputation. For example, a company might be concerned with: board of directors/shareholders, investors, stock analysts, clients, employees, suppliers/subcontractors, financial institutions, opinion leaders, insurance company, unions, media, regulators and action groups. When a crisis occurs, one should identify key companies within each audience that might be affected. An employee must then contact a key influencer within those firms. The ideal candidate is someone who has an existing relationship with the influencer.

•**Appoint a media spokesperson.** Selecting a spokesperson is critical. If a company does not understand how to communicate with the media, it will likely receive poor coverage. This person should be named and trained before a crisis occurs.

•**Deliver a buy-time statement.** A crisis, particularly an event that involves human life, generates chaos, which in turn creates an urge to stonewall the media. This response should be avoided because it screams "guilty as charged." A company's best interests are served when it is depicted as being responsive. This does not mean "divulge everything"; rather, a company should deliver a "buy-time statement" which shows it will not run and hide, nor will it release unverified information. A sample buy-time statement: "My name is (name) and I am (title) with (company). The incident has just happened and I am not prepared to answer any questions at this time. Please stay in this safety area so we can do our job and take care of the situation. I need to return to the site, but either (spokesperson) or I will be back at (time) with an update."

•**Deliver additional statements.** As information is verified, the company can develop a more-detailed statement. It should be brief and concise in order to minimize the possibility of misinterpretation. It should:

•Acknowledge the incident, but not discuss possible cause.

•Express concern for any victims and their families.

•Communicate how the company is responding.

•Advise when the next update will be available.

•**Prepare for a media interview.** An interview will be more successful if the spokesperson has addressed the following issues before speaking to the reporter(s):

•*Determine the communications goal of the interview.* For example, a company may want to demonstrate its determination to discover the cause of the incident and concern for those affected.

•*Develop a mantra for the spokesperson.* This statement helps the spokesperson survive the rough segments of an interview. For example, if s/he does not know the answer to a question, s/he could say, "I don't know but I will investigate and will get back to you by (time)."

•*Anticipate questions.* A successful interview depends on anticipating questions (including "ugly" ones) that may be asked, developing responses and rehearsing their delivery.

•**Crisis aftermath.** Keep lines of communication with employees and other audiences open until the crisis has quieted. The spokesperson should be prepared for a reporter to call at any time with queries relative to the incident. Statements should be brief, succinct and consistent.

Never doubt the power of the media to influence public opinion. A mobilized public can shut down a firm that does not respect this power. A well thought out communications plan will prevent such an outcome.

Janine Reid *is the founder of the Janine Reid Group Inc. in Denver. She is the author of two books on crisis management planning, and has also produced two videotapes on crisis management and working with the news media.*

Figure 1

Risk Assessment Matrix

	High Severity	Moderate Severity	Low Severity
High Frequency			
Moderate Frequency			
Low Frequency			

raw materials since a smaller pool of resources is available should deliveries be suspended.

Potential downtime for each critical business function must be estimated in order to properly assess the risk and establish priorities for recovery efforts. A business impact analysis (defined by *Disaster Recovery Journal* as "the process of analyzing all business functions and the effect that a specific disaster may have upon them") should be completed. "Critical" business functions can be thought of as those functions absolutely necessary for the business to remain in operation. This will vary from business to business, but could include items such as computer and/or phone capability, the ability to collect accounts receivable or the ability to manufacture a product. Noncritical business functions could include word processing, housekeeping, preventive maintenance and stocking of amenities.

As part of this phase, budgets must be created for mitigation measures. The cost-benefit relationship must be included in the decision-making process. Mitigation measures may result in risks being downgraded from a frequency and/or severity standpoint.

Awareness of certain risks will be heightened by global, regional or local events. For example, plans are typically upgraded following a significant earthquake (e.g., the 1994 Northridge, CA, quake). Following Sept. 11, 2001, many crisis management plans were reviewed and modified in order to address terrorism. As management perception of a problem inevitably fades, it is more difficult to retain emphasis on a particular subject. In his 2001 Chairman's Letter to Shareholders of Berkshire Hathaway Inc., Warren Buffett said, "Fear may recede with time, but the danger won't. The war against terrorism can never be won. The best the nation can achieve is a long succession of stalemates." Similar statements could be made with respect to other risks. Crisis management planners must take advantage of heightened management interest.

Crisis Planning & Preparation

The crisis management plan must be in writing and must address each issue identified during the identification and assessment phases. It must also clearly define roles and responsibilities. If a crisis occurs and multiple people attempt to take control of the situation, confusion will result at the scene. Many emergency plans likely already exist within a company, so rather than reinvent the wheel, it is best to scrutinize such plans to assess their adequacy.

Evaluation of existing control or mitigation measures is part of the initial risk assessment process. Improving these measures is part of the crisis preparation process. A crisis that does not occur as a result of proper preventive activities saves an organization time and money. Plans should include a range of information such as:

- incident command system (ICS) structure;
- emergency operations center (EOC) location and backup location with instructions for team members to assemble at the backup location when the primary location is not available;
- emergency response team structure, roles and responsibilities;
- requirement for team members to maintain copies of the most recent plan in multiple locations that would not be subject to the same incident;
- detailed diagrams including access roads, buildings, surrounding structures, utility lines and control valves;
- a defined contact for working with responding governmental agencies;
- mutual aid agreements or contracts that allow access to preferred vendors;
- details on identified risks, control methods for those risks and response actions required following an event;
- communication procedures during and after the crisis, including notifying the emergency response team and communicating with employees, employee family members, suppliers, vendors, shareholders and the press; this document should include an off-site emergency phone number for messages (preferably an 800 number shared with all employees) and procedures for updating the recording; equipment could include telephones, cell phones, radios, messengers, pagers and emergency alert systems;
- location of all emergency response equipment and supplies, including maps, first-aid kits, fire extinguishers, AEDs, cell phones and radios, food and water provisions;
- search and rescue procedures;
- provisions for backing up data and accessing vital records, as well as contingencies for hardware, software and paper records;
- contingencies for plan failures, particularly with respect to alternative power sources, communication methods/equipment and provision of medical services;
- employee training;

Role of HR in Crisis Management

By William J. Coy

At its best, human resources is an active strategic partner that monitors, articulates and supports the roles, relationships, boundaries and expectations of an organization. Like no other time, a traumatic event requires a reframing and a reinforcing of all of these variables. Before, during and after an event, HR should be a significant partner—if not a prime mover of organizational response.

Before the Event

•**Acknowledge that it can happen.** The first step is awareness. A company must be willing to think and plan around some unpleasant realities.

•**Predetermine roles and resources.** Who will do what? What resources will those people have at their disposal?

•**Know line of authority and contacts.** Who holds primary responsibility for management and coordination of response?

•**Train staff.** Train staff in response and anticipation of the impact of trauma.

•**Make contact with the EAP representative.** Memorize the number. The time to establish the working relationship with the EAP is well before it is needed.

•**Run scenarios.** Anticipate what can go wrong and perform realistic response scenarios. Grade the response, plan and improve it.

After the Event

•**Check in with employees.** What do they need? The more choices and power a firm can give workers in a post-trauma situation the better. Care must be taken to ensure that feelings of powerlessness are not reinforced. For example, do not unilaterally decide that everyone must go home or must stay. Offer choices. People cope in their own ways.

•**Communicate with employees.** Nothing should be more carefully crafted than employee communication. It should acknowledge the reality, without being harsh or understated. It should also convey an appropriate amount of compassion and empathy, while presenting a voice of confidence and leadership.

•**Additional resources.** Many employers have EAPs that provide counseling, critical incident stress debriefings, referrals and management assistance in dealing with post-trauma stress.

•**Time off.** Trauma can be a major disruption to the psychological, physical and emotional well-being of individuals. Some might need time away from work. Monitor performance and reaction, and allow as much latitude as possible in this regard.

William J. Coy *is a management consultant with La Piana Associates. Prior to this he was director of human resources with Yosemite National Institutes. During his tenure in that position, an instructor and three other people were murdered in the park. Coy's post-tragedy role was to coordinate a response by the organization and the management team, and tend to the needs of staff, management and families.*

•psychological evaluations for crisis management team members;

•psychological counseling for employees following a crisis;

•provision for emergency funding of activities (FEMA).

Public agencies often provide substantial support during the response. Understanding what level of support such agencies can provide for given types of emergencies is part of the planning stage. The support available depends on many variables, including the nature of the crisis, the agencies' capabilities and the nature of a business. Public agency support could be in the form of firefighters to help control a fire, a HazMat team to address a chemical spill or an ambulance with medical care providers. A large-scale flood may result in the involvement of the Federal Emergency Management Agency (FEMA) whereas a small flood may not. A police department with a trained bomb squad might respond differently to a suspicious package than one without specialized training. A hospital may receive better assistance than a retail store in a similar crisis because assisting the hospital might be considered a greater public service.

Pre-incident planning for specific issues may include:

•**Evacuation procedures.** Procedures could describe how to call for an evacuation; how to ensure everyone exits; how to shut down critical equipment; and where to gather following evacuation. Diagrams could include designated exits (at least two remote exits from every location); gathering points (where and to whom to report); first-aid supplies and fire protection equipment; electrical circuit breakers, and gas and water control valves.

•**Earthquake.** The plan could include seismic upgrades for the facility, educating employees on actions to take during and after an earthquake, and providing emergency supplies.

•**Fire.** The plan could cover alarm systems/procedures, firefighting equipment, evacuation procedures and employee training on firefighting techniques.

•**HazMat incident.** A plan could include alarm systems for notifying the response team or signaling an evacuation; procedures for isolating the spill or contaminated area; procedures for notifying the fire department or EPA; and policies on cleanup and disposal of material.

•**Workplace violence.** The plan could include awareness training, de-escalation training, self-defense, response protocols and emergency notification procedures.

Once plans are developed, appropriate personnel must be trained, with refresher training provided on a regular basis. Written plans, particularly contact names and phone numbers, should be reviewed and confirmed.

Emergency contact names and phone numbers may include: alarm company, ambulance service, attorney, bomb squad, building inspector, crisis counselors, demolition service, utility companies, EPA, fire department, guard service, HazMat cleanup, hospital and medical care providers, insurance broker, kidnap and ransom specialists, media, OSHA, poison control center, police, Red Cross, sprinkler contractor, suppliers and vendors (IIA). This review should be completed by the crisis management plan coordinator and anyone with specific responsibilities set forth in the plan.

After plans are prepared and training has been conducted, the risk identification and risk assessment phases must be revisited regularly. Businesses continually change, which may necessitate revisions to the crisis management plan.

Crisis Mobilization & Response

The response phase begins once an incident has occurred or a warning suggests an incident may occur soon. Mobilizing personnel and responding properly will help minimize business disruption. Therefore, having a well-trained, team is crucial.

One pressing issue during this phase is ensuring that people know their responsibilities and have the authority to act. This includes a succession protocol if key personnel are not available. These issues are defined during the planning process and are included in the incident command system structure. Establishing alternate worksites may be important if a location is rendered unusable or hazardous. Arrangements for such sites should be considered during the planning phase.

Crisis management plans will never address all specific risks. New risks may be identified or become more apparent over time. Therefore, personnel must be trained to be flexible so they can use common knowledge to respond to an unplanned situation.

Recovery

Once a business has responded to the immediate crisis, it must deal with recovery of normal operations. Recovery priorities and plans for varying lengths of downtime should be addressed in the established plans. Maintaining regulatory compliance during recovery is important as well. For example, employees must be protected with appropriate PPE. They must also be trained how to respond to various situations. Improper response—such as spraying water on a HazMat spill—may create a larger problem than no response at all.

The recovery phase is often completed without assistance from public agencies such as fire and police departments (they typically leave after the initial response). Each organization must determine how to respond. Some go out of business, while others implement fully developed plans and recover quickly.

Restoring critical functions at the crisis site or an alternate location is the first step. Once this occurs, other business functions can be restored. As noted, what is critical for one business may not be critical for another. In many cases, decisions must be made about rebuilding, repairing or refurbishing buildings and equipment. This will vary depending on the nature of the event and resources available.

Beyond dealing with buildings and equipment, a crisis poses psychological

The Legal Perspective

By Fred Walter

As soon as a crisis occurs, investigations to assign responsibility begin. Many agencies and interest groups will ask the fundamental questions of who, what, when, where and why. Local agencies such as fire and police will investigate. The media will assert the public's right to know. Regional and state agencies will arrive as well. And don't forget about the insurance companies and attorneys for any injured workers and third parties. Clearly, managers' corporate and personal vulnerability to civil and criminal litigation and administrative penalties is greater than ever before.

Without early attention to the organization of crisis response, a company's SH&E professional's goals may quickly diverge from its attorney's. SH&E professionals and other experts are trained to analyze root causes of incidents. To do so, they immediately start gathering facts—photographs, diagrams, documents and witness statements. They put working hypotheses about what might have occurred (sometimes called "cut sets") on paper, to be revised as new information is received. They summarize findings and likely scenarios of cause in notes or memos. Their purpose is to say, with some degree of certainty and as soon as possible, what caused the event and how systems or procedures should be changed to prevent similar occurrences. Their training also instills in them a collegial spirit that supports the ethic of sharing information so that others may use it to prevent similar events.

All of this is good. All of this also makes attorneys nervous. In the uncertainty of the aftermath, management hires attorneys to do two things: 1) inform the company of its potential liabilities, and the pros and cons of alternative courses of action; and 2) limit, to the extent possible, the company's potential liability in any forum in which it might find itself. To do this, attorneys are trained—much like SH&E professionals—to learn as much as they can as soon as possible. They also analyze all evidence retrieved. But they ask different questions. Is this fact friend or foe? How could this fact be used against the client? How soon am I likely to be required to disclose this document/statement/photograph/lab report to a foe?

Attorneys also are conditioned to not share with others until they must. They are taught that the party which controls information the longest usually gets the best result. This does not mean withholding or burying information forever; modern discovery rules prevent that. Instead, attorneys play a tactical game, protecting clients by maintaining control over the rate of the release of information and the context in which it is disclosed. Unless the information gathered in an investigation can be effectively protected, everything that is gathered, from photographs to lab samples, from written statements to brainstorming notes speculating why the event occurred, is fair game for subpoena in any later court litigation or administrative hearing process.

Two legal privileges against disclosure help attorneys and clients protect information developed during an investigation. The attorney work product privilege protects information developed by an attorney and his/her investigators (including SH&E professionals). While not fully effective, this privilege can usually protect an investigator's written notes and impressions. The attorney/client communication privilege protects exchanges of information between these two parties and their affiliated representatives.

Management attorneys must be especially sensitive about signed witness statements. While such statements created just after a traumatic event might preserve the writer's memory better than on a later day, they will likely be charged with emotion. It is natural for near-victims to feel some degree of guilt after an incident; today's emotionally based speculations (if only I had . . .) can quickly become tomorrow's admissions against interest.

Attorneys also are concerned about expert's written reports. One person's hypothetical scenario is another's speculation. Once made public, it is hard to pull back, even if a particular hypothesis is later discounted by new information.

The best results are achieved by assigning an attorney to direct and supervise the investigation as early as possible. Once legal privileges are properly established and with the company's attorney as a team member, the experts can continue their work and speak freely, leaving any worries about the ramifications of their findings to the attorney.

Fred Walter, Esq., *is a Healdsburg, CA, lawyer who represents management in OSHA and related matters. To date, he has supervised seven workplace crisis responses and investigations.*

Crisis Management Survey Results

1) What best describes your industry?

A) Insurance	11.5%
B) Manufacturing	37.2%
C) Hospitality	0.0%
D) Retail	1.7%
E) Construction	12.5%
F) Other	37.2%

2) How many employees are there in your company?

A) Less than 100	8.4%
B) 100 to 500	23.0%
C) 500 to 1,000	15.9%
D) More than 1,000	52.7%

3) Do you have a formal (written) crisis management program?

A) Yes	90.5%
B) No	9.5%

4) Have you implemented your plan in the past 12 months in response to a real crisis?

A) Yes	32.4%
B) No	67.6%

5) If you implemented your plan in the past 12 months, describe the crisis.

Representative types of crises identified included:

- Bomb scare/threat
- Bridge/highway collapse
- Cattle infection
- Chemical fire
- Civil disturbance by protestors
- Earthquake
- Emergency medical intervention
- Fatal accident
- Fire in adjacent building
- Fire at client facility
- Hazardous chemical spill
- Hurricane
- Ice storm
- Labor unrest
- Liquid ammonia leak
- Loss of employees, workplace, data due to Sept. 11 events
- Masonry wall collapse
- Oil spill
- Opening mail following anthrax scare
- Passenger train derailment
- Restructuring of facility staffing
- Security needs following Sept. 11
- Snow storm
- Tornado
- Total failure of power plant
- Workplace violence
- World Trade Center collapse

6) How many facilities/locations are covered by the plan?

A) 1	27.7%
B) 2 to 5	20.9%
C) 5 to 10	9.8%
D) More than 10	41.6%

7) If you have facilities outside the U.S., are those facilities covered by your plan?

A) Yes	19.6%
B) No	27.4%
C) N/A	53.0%

8) Which department is responsible for the plan?

A) Risk management	11.8%
B) Executive management	18.6%
C) Safety	49.3%
D) Facilities	6.4%
E) Other	13.9%

9) What name does your company use for the plan?

A) Crisis management plan	18.9%
B) Business continuity plan	6.1%
C) Emergency response plan	62.8%
D) Disaster plan	4.7%
E) Other	7.4%

10) Are temporary workers and contractors included in the plan?

A) Yes	81.1%
B) No	18.9%

11) When was your plan last updated?

A) Within 6 months	55.1%
B) Within 12 months	25.3%
C) Within 24 months	9.5%
D) Never (not since the plan was written)	10.1%

12) How often are crisis mock drills held?

A) Every 6 months	20.6%
B) Every 12 months	44.6%
C) Every 24 months	6.8%
D) Never	28.0%

13) Is the safety manager directly involved in the planning process?

A) Yes	87.2%
B) No	12.8%

14) How did you determine which crises you would develop plans to address?

A) Addressed only common crises such as fire, flood, earthquake, tornado, bomb threat	33.8%
B) Addressed common crises plus others that the company has experienced in the past	30.1%
C) Addressed crises recommended by insurance carrier, broker, or consultant	5.1%
D) Conducted brainstorming sessions to identify potential crises	31.1%

15) Have all crisis management plans been implemented?

A) Yes	64.5%
B) No	35.5%

16) How would you characterize the level of your company's preparedness since the build up to Y2K?

A) Better than before Y2K	64.2%
B) The same as before Y2K	34.5%
C) Worse than before Y2K	1.4%

17) How would you characterize the level of your company's preparedness since the events of Sept. 11?

A) Better than before Sept. 11	52.4%
B) Same as before Sept. 11	46.6%
C) Worse than before Sept. 11	1.0%

18) How was your plan primarily developed?

A) Using internal resources	76.0%
B) Using insurance company resources	3.7%
C) Using insurance broker resources	1.0%
D) Using outside consultant resources	14.5%
E) Using Internet resources	4.7%

19) Have all crisis management team members been provided training on your plan?

A) Yes	67.9%
B) No	32.1%

20) Have key team members been provided media training?

A) Yes	61.8%
B) No	38.2%

21) Do you have a formal plan for providing post-crisis trauma counseling for your employees?

A) Yes	62.2%
B) No	37.8%

22) Do you have preferred vendors established to respond following a crisis?

A) Yes	66.2%
B) No	33.8%

23) How would you learn about new threats and how to respond to them?

A) Attending seminars	15.9%
B) Reading newsletters or professional publications	48.3%
C) Conducting research on the Internet	12.5%
D) Getting information from insurance contacts or outside consultants	23.3%

aspects that should be addressed, yet are often neglected. Recovery teams are often subjected to physical and mental demands that can produce depression, fatigue and poor decision making. Counseling for team members and other employees, particularly witnesses, should be made available; these services should be arranged during the planning phase.

The recovery process can be facilitated by insurance policies, public agencies and private relief organizations. For example, insurance policies can pay for direct damage to buildings or equipment; injuries to personnel; damages caused to third parties; direct and contingent business interruption losses and expediting expenses; and other costs. An organization's ability to rely on financial protection from the insurance company depends on the type and scope of policies written and exclusions included in them. Aside from ensuring that the proper types of coverage are in place, appropriate insurance limits must be established. This is particularly important for property policies with coinsurance provisions. Such policies may require insurance limits at 80, 90 or 100 percent to value with penalties after a loss if limits are inadequate. Guaranteed replacement costs policies are different from actual cash value policies. Insurance policies cannot, however, ensure the recovery of operations nor can they prevent customers from going to a different provider.

Insurance protection is only part of the equation. According to the Liberty Mutual Workplace Safety Index, "When the indirect costs of workers' compensation claims are added to the $38.7 billion in direct [injury] costs . . . the total economic burden of workplace injuries and illnesses is far greater, with estimates ranging between $125 billion to $155 billion" (Liberty Mutual Reseach Center, Feb. 26, 2001). This shows that indirect costs are three to four times higher than direct costs.

Public agencies and relief organizations may provide housing, medical assistance, financial grants and low-cost loans to affected organizations and their employees. For example, following the World Trade Center collapse, emergency service personnel, American Red Cross and FEMA provided assistance, while private organizations provided aid in the form of communication equipment, food and water, and cash grants. The eventual recovery of most individual businesses was left to the businesses themselves.

Plan Testing

Once a plan has been established, exercises must be conducted to verify that it works well. Training simulations/exercises need not be held for all contingencies, but they must involve key decision-making personnel. Just because a senior executive has assumed responsibility for leading the team does not mean that executive will perform adequately in the event of a crisis. Training simulations help identify who will respond well to a crisis.

Public agencies expected to respond to a crisis should be involved in these exercises as well. Many fire departments and police departments become involved, and their input is essential. When the plan is tested through a simulation or a real-life crisis, deficiencies will often be noted. A "lessons learned" or "mistakes made" meeting should be held to identify corrective actions to improve the plan.

Conclusion

Crisis management planning is a complex subject that requires a multidisciplinary approach. Many resources are available to help organizations develop these plans. If done correctly, developing a plan is a time-consuming process that thoroughly evaluates and quantifies risks and provides a framework for response. Each plan will be unique to the business entity that develops it. Business decisions must be made with respect to risks to be retained and risks to be insured. Control measures can be implemented, but risk cannot be eliminated. Proper planning and effective response can significantly minimize the impact of a crisis on any business. ■

Exercises must be conducted to verify that the plan works well. Training exercises need not be held for all contingencies, but they must involve key personnel.

References

American Chemistry Council (ACC). *Site Security Guidelines for the U.S. Chemical Industry.* New York: ACC, 2001.

Boytor, S. "Risk Assessment: Solving Day-to-Day Problems, Part II." *Proceedings of the 2001 ASSE Professional Development Conference.* Des Plaines, IL: ASSE, 2001.

Buffett, W. "2001 Chairman's Letter to Shareholders." Omaha, NE: Berkshire Hathaway Inc., Feb. 28, 2002.

Cox, J. and W. Hawthorne. "Crisis Management: Are You Really Prepared?" *Risk Management/Insurance Div. Newsletter.* Fall 1999.

Federal Emergency Management Agency (FEMA). *Emergency Management Guide for Business & Industry.* Washington, DC: FEMA, 1996.

Grimaldi, J. and R. Simonds. *Safety Management.* 5th ed. Des Plaines, IL: ASSE, 1993.

Insurance Institute of America (IIA). *Essentials of Risk Control.* 3rd ed. Vol. 1. Malvern, PA: IIA, 1998.

Irby, D. and A. Land. "Disaster Planning & Fire Safety." *Occupational Health & Safety.* Nov. 2001: 28-30.

Jones, R. "Anticipating the Worst of Times." *Security Management.* April 2001: 42.

Main, B. "Risk Assessment: Solving Day-to-Day Problems, Part I." *Proceedings of the 2001 ASSE Professional Development Conference.* Des Plaines, IL: ASSE, 2001.

Morganti, M. "A Business Continuity Plan Keeps You in Business." *Professional Safety.* Jan. 2002: 19, 56.

National Safety Council (NSC). *Accident Prevention Manual for Business & Industry: Administration & Programs.* 10th ed. Itasca, IL: NSC, 1992.

Reid, J. *Crisis Management: Planning and Media Relations for the Design and Construction Industry.* New York: John Wiley & Sons Inc., 2000.

Your Feedback

Did you find this article interesting and useful? Circle the corresponding number on the reader service card.

RSC#	*Feedback*
25	Yes
26	Somewhat
27	No