

THREE

Auditing an
Organization's CM
Strengths and
Vulnerabilities

WHAT TO DO BEFORE
AND AFTER A CRISIS

A paradox is associated with CM: We cannot understand fully what we need to do during crisis unless we first understand what we need to do and have in place before a crisis; at the same time, we can not understand fully what we need to do beforehand unless we understand what we will be required to do during a crisis. There is no easy way out of this. The best that we can do is work back and forth between these two critical phases so that over time, executives and their organizations become better prepared.

After every crisis or near crisis, a postincident audit should be conducted (see Figure 2.9, Point 54). The purpose of such audits is to help an organization review what it did well and learn what it needs to improve on so that it will be better prepared to face its next crises (Boxes 54–57). Although such reviews are essential, many organizations do not bother with them and hence are not well prepared to face their next crisis (Box 58).

THE PRE- AND POSTCRISIS AUDIT

Figure 3.1 is an overview of the activities comprising a thorough CM audit. It does not distinguish between a precrisis and a postcrisis audit.

A Precrisis Audit

A precrisis audit typically includes interviews with the key members of an organization's corporate staff and/or the key members at a particular plant or site. The interviews should be designed to probe for four critical factors that lead an organization to be either CM prepared or CM prone. A sample set of interview questions is given in Table 3.1.

The same questions are asked of every top executive on an organization's corporate staff, so as to identify common perspectives as well as significant differences. Determining an organization's CM strengths and weaknesses is too important to be left to the judgment of a single person; all senior executives should participate in such evaluations.

In addition, you cannot find the information necessary to determine an organization's CM strengths and weaknesses solely by studying its CM manuals, documents, training programs, and so forth. Although such sources are a valuable source of infor-

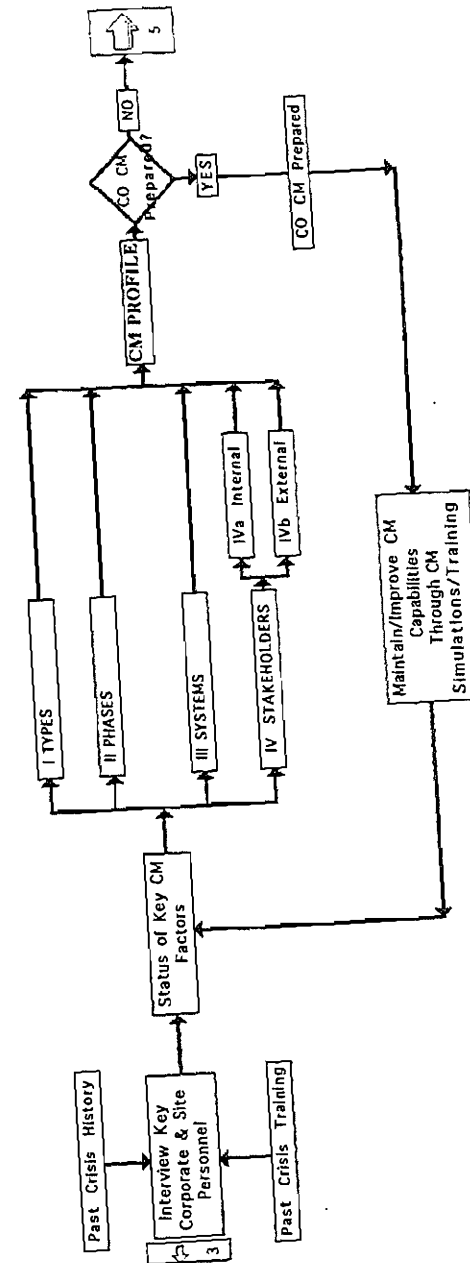


Figure 3.1. Precrisis and postcrisis audits.

TABLE 3.1. CRISIS MANAGEMENT AUDIT GUIDE

The following questions indicate the general kinds of issues that should be raised in an interview. These questions may also be used as a general guide to explore certain issues further.

1. What is your definition of a crisis for your organization?
2. In your opinion, what kinds of crises is your organization prepared for, and why?
3. What kinds of crises is your organization not prepared for, and why?
4. Does your organization have a crisis management team (CMT)?
 - a. If your organization has a CMT, are you a member of it?
 - b. Who else is on the CMT?
 - c. What kind of training, if any, has your team been given?
 - d. Has your team undergone conflict resolution training?
5. What kinds of early warning systems, or signal detection mechanisms (SDM), for crises does your organization have?
 - a. For which crises?
 - b. Are the SDMs integrated?
 - c. Are they dispersed throughout your organization?
6. Is the detection of crises specifically rewarded?
7. Is probing for crises discretionary or mandatory, and is it rewarded?
 - a. Do you conduct formal training sessions or simulations for crises? If so, for what kinds of crises?
 - b. How frequently?
 - c. What do the sessions specifically test for?

TABLE 3.1. (continued)

- d. Do they probe for and uncover key, taken-for-granted assumptions?
8. Describe the kinds or ranges of damage containment mechanisms your organization has.
 - a. For which kinds of crises?
 - b. How frequently are they inspected or maintained?
 - c. How frequently are they reviewed for design flaws?
9. Describe your organization's business recovery and/or backup systems.
 - a. For which kinds of crises?
10. Does your organization have formal backup systems for computer and telecommunication systems?
 - a. Does your organization have both "hot" and "cold" storage sites?
11. Does your organization conduct formal review sessions of past crises and near crises, not to blame individual people but, rather, to improve its ability to prevent and respond better to future crises?
12. Describe the state of your organization's primary technologies.
 - a. Are fault-tree analyses performed in regard to probable failure modes?
 - b. Are formal risk and assessments performed?
13. How do the following characteristics of your organization contribute to the prevention or cause of crises?
 - a. Formal organizational structure?
 - b. Job descriptions?
 - c. Reward mechanisms?
 - d. Formal and informal channels of communication?
 - e. Authority/power structure?

TABLE 3.1. CRISIS MANAGEMENT AUDIT GUIDE (continued)

14. Have human factor analyses been performed with regard to how operators and maintenance personnel can cause or prevent crises?
15. Describe the general culture or mind-set of your organization.
 - a. What denial mechanisms or beliefs hinder effective crisis management?
 - b. Does the general culture or mind-set of your organization contribute to effective CM?
16. What stakeholders are explicitly considered in the formation and execution of CM plans and procedures?
17. What are your organization's CM capabilities? What evidence do you have to back up your beliefs?
 - a. How well do these capabilities match your organization's crisis plans?
18. Is CM tied into or integrated with other key programs such as
 - a. Total quality management (TQM)?
 - b. Environment?
 - c. Health and safety?
 - d. Ethics?
 - e. What else?
19. Is CM part of everyone's job?
 - a. Why?
 - b. Why not?

mation, at some point you should talk to people to find out what CM means to them and how they view their organization's CM preparedness.

Because these interviews are such an important part of the CM audit, we recommend that they be conducted by outsiders who have been specially trained to conduct and analyze interviews. Furthermore, the interview will not yield valuable information unless strict confidentiality and anonymity are guaranteed, and insiders generally cannot provide such assurances. The interviewer must be able to reassure those being interviewed that under no circumstances will the responses of individuals be identified, that only aggregate data will be given to the organization for consideration.

We usually interview the following people in order to compile a collective portrait of an organization's CM strengths and weaknesses: (1) chief executive officer, or CEO; (2) chief financial officer, or CFO; (3) chief operating officer, or COO; as well as the most senior executive in charge of (4) security, (5) human resources, (6) health and safety, (7) environment, (8) corporate communications and public affairs, (9) government affairs, (10) public relations, (11) quality assurance, (12) head of management information systems, (13) ethics officer, (14) corporate training, and (15) head of technical operations.

The interview questions (Table 3.1) explore four factors that have been shown to play a significant role in crises: (1) types, (2) phases, (3) systems, and (4) stakeholders.¹ *Types* refers to the kinds (scope, breadth) of crises for which an organization is prepared, as well as the reasons for selecting those particular crises. *Phases* refers to how well an organization is prepared to detect, contain, recover from, and learn from crises. *Systems* refers to how well an organization is prepared to manage the complex systems that can either cause or prevent a crisis. Finally, *stakeholders* refers to the critical parties, including both individual people and institutions, who would be affected by a crisis or who could affect the organization's ability to manage a crisis.

Generally, the results of a CM audit are presented in several forms: (1) a written report that summarizes the major findings and makes recommendations for improvement, (2) an on-site oral presentation of the results, and if possible, (3) a CM profile that shows graphically an organization's CM strengths and weaknesses with regard to the preceding four factors. Figure 3.2 shows whether an organization is performing poorly, questionably, or well on each of these four factors. Because Figure 3.2 is part of the software

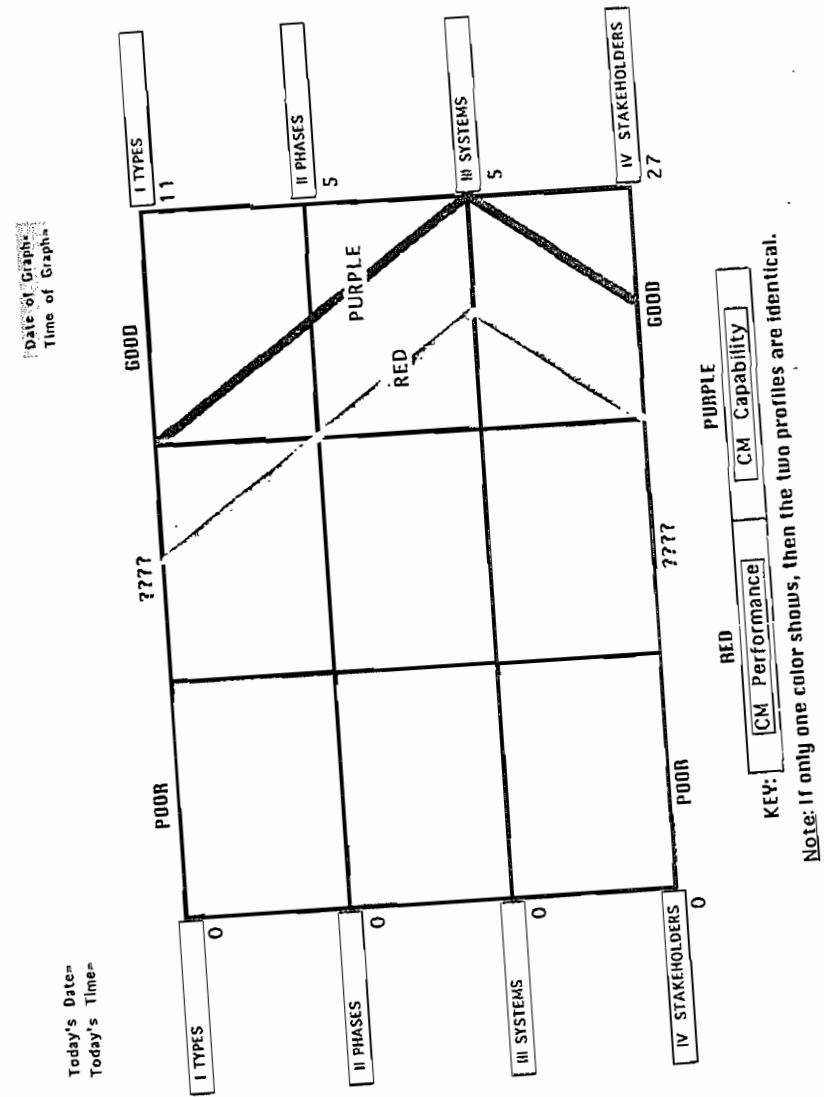


Figure 3.2. A CM profile showing an organization's CM strengths and weaknesses.

package CrMgt, we shall discuss it in more detail in Chapter 5. One of the strengths of CrMgt is that it allows the user to evaluate quantitatively the CM strengths and weaknesses of his or her organization. The software package also automatically plots a graph like the one shown in Figure 3.2.

A CM profile is one of the principal outputs of the CM audit process shown in Figure 3.1 and is indicated by the box in Figure 3.1 labeled CM PROFILE. An organization's CM strengths and weaknesses are used to determine whether or not the organization is CM prepared, as shown on the right side of Figure 3.1. If an organization is judged to be CM prepared, it is not an excuse for relaxing. Rather, the box at the bottom of Figure 3.1 is meant to indicate that an organization must continue to work hard to maintain and improve its CM capabilities through constant simulations and training.

A Postcrisis Audit

A postcrisis audit differs from a precrisis audit in several respects. First, the chief goal of the postcrisis audit is to identify lessons to be learned from a particular "trigger" event and how best to integrate those lessons into an organization's daily operations and CM practices. Second, a postcrisis audit is prompted

by a particular crisis or near crisis. Third, it focuses principally on that event and only secondarily on an organization's overall crisis preparedness.

Like a precrisis audit, a postcrisis analysis concentrates on the four factors that play a significant role in virtually all crises: (1) types, (2) phases, (3) systems, and (4) stakeholders. Because of the specificity of postcrisis audits, it is difficult to construct a general audit guide, but there are important areas that should be covered:

1. What happened? Determine the basic facts (disputed and undisputed).
2. What caused the incident.
3. Which factors (internal and external to the organization) led to this type of occurrence? Did the structure, culture, technology, or people in the organization contribute to the crisis potential? Did the business environment or pressure from external stakeholders create or exacerbate the organization's vulnerability to this type of crisis?
4. When responding to the crisis, what was done well?
5. What was done poorly?
6. Does the organization continue to be vulnerable to this type of crisis?

7. Could a crisis of this type lead to other crises? What are they?
8. What steps must the organization take to reduce its risk to future crises, both this type and others?

As with precrisis audits, it is desirable to interview the broadest possible range of executives, managers, and employees with knowledge of the incident and also those affected by it. External stakeholders should be interviewed whenever possible, as the perspective of those outside the organization is often different from that of insiders and can reveal important information that might otherwise go unnoticed.

Although no two crises are the same, identifying the specific nature of a crisis and its causes is necessary in order to understand the organization's vulnerability to that general type of crisis. The contributing factors are equally important because they provide clues to structural weaknesses that may make an organization susceptible. Analyzing an organization's response is also a good way to identify the systems and stakeholders at risk from a particular type of crisis.

One of the most difficult aspects of CM is integrating the lessons learned from crises and near crises. When conducting a postcrisis audit, it is helpful to secure a commitment in advance to use the audit

findings for future improvement. This requires a willingness by the organization to engage in "no-fault" learning. Although this is difficult, in our experience, it is precisely this commitment to no-fault learning that distinguishes successful postcrisis audits from pro forma exercises.

THE FOUR MAIN FACTORS OF CM







Figures 3.3 through 3.9 illustrate the kinds of issues that are associated with the four main CM factors: (1) types, (2) phases, (3) systems, and (4) stakeholders. Although we will consider each figure, we will not discuss every aspect of them at this point. (The figures are also part of the software package CrMgt, which is used to determine an organization's CM profile. For this reason, the figures ask the user to make various judgments that are scored automatically. The scores are then used to compare an organization's performance during a crisis with its preparation or capabilities before the crisis.)

Types

Since both the numbers and the different forms that each crisis assumes are unlimited, no organization,

even with the best of resources, can plan for every possibility. Furthermore, no crisis ever happens exactly as expected. Therefore, CM plans should not be considered as ends in themselves; instead, they should be considered part of the process of thinking about and training for the “unthinkable.”

Figures 3.3 and 3.4 show eleven basic types of crises as well as examples of the various possible subtypes. It is important to understand that we are not claiming that these, and only these, eleven exhaust all possible kinds of crises. Instead, Figures 3.3 and 3.4 identify, to the best of our current knowledge, the variety of possible crises. We have found from previous research that crises fit into eleven groups or families, those listed in Figures 3.3 and 3.4.² Our research has also shown that the “best,” or CM-prepared, organizations do not prepare for just one kind of crisis. Instead, they prepare for a variety of crises; in effect, they compile a *crisis portfolio*, by preparing for at least one type of crisis in each of the eleven categories. They also do not get sidetracked over precisely which subtype they should prepare for. Rather, they understand that even though they are not identical, the different subtypes in a particular category are similar. In addition, because no crisis ever happens exactly as expected, it does not matter






MAIN TYPES	SUBTYPES	CURRENT CRISIS ANY of the SUBTYPES?	AT LEAST ONE SUBTYPE in CM PLAN?
1  Criminal Attacks	1. Copycats 2. Employee Violence 3. Product Tampering 4. Sabotage 5. Sexual Harassment 6. Terrorism	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> DON'T KNOW	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> DON'T KNOW
2  Economic Attacks	1. Boycotts 2. Hostile Takeovers 3. Stock Devaluation 4. Strikes	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> DON'T KNOW	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> DON'T KNOW
3  Loss of Proprietary Information	1. Fake Rumors 2. Copyright Infringement 3. Counterfeiting 4. Proprietary Information	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> DON'T KNOW	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO <input type="checkbox"/> DON'T KNOW
4  Industrial Disasters	1. Major Contaminations 2. Major Explosions 3. Major Fires 4. Major Releases 5. Major Spills	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> DON'T KNOW	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO <input type="checkbox"/> DON'T KNOW
5  Natural Disasters	1. Bizarros 2. Earthquakes 3. Electrical Storms 4. Floods 5. Hurricanes 6. Typhoons	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> DON'T KNOW	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO <input type="checkbox"/> DON'T KNOW
6  Breaks in Equipment & Plants	1. Computer Breakdowns 2. Distribution Net Defects 3. Major Operator Errors 4. Major Product Defects 5. Major Product Recalls 6. Major Plant Defects 7. Security Breakdowns 8. Telecommunications Breaks 9. Quality Defects	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> DON'T KNOW	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO <input type="checkbox"/> DON'T KNOW

Total CM Performance
Score=4

Total CM Plan
Score=7

0=Poor.....11=Excellent

Figure 3.3. The eleven types of crises and their subtypes.

MAIN TYPES	SUBTYPES	CURRENT CRISIS ANY of the SUBTYPES?	AT LEAST ONE SUBTYPE in CM PLAN?
7 Legal 	1. Major Corporate Lawsuits 2. Major ClassAction Suits 3. Major Distributor Suits 4. Major Officer Liabilities 5. Major Product Liabilities 6. 7.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> DON'T KNOW	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> DON'T KNOW
8 Reputational Perceptual 	1. Damaging/Fakes Rumors 2. Damage to Reputation/Logo 3. Projection onto Brand/Logo 4. 5. 6. 7.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> DON'T KNOW	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> DON'T KNOW
9 Human Resources Occupational 	1. Employee Violence 2. Executive Succession 3. Family Violence 4. Faulty Corporate Culture 5. Sexual Harassment 6. 7.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> DON'T KNOW	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> DON'T KNOW
10 Health 	1. AIDS 2. Environmental Contamination 3. Jobrelated Injuries 4. Jobrelated Deaths 5. 6.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> DON'T KNOW	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> DON'T KNOW
11 Regulatory 	1. Adverse CO Regulations 2. Adverse Special Interests 3. Adverse Industry Regulations 4. 5. 6.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> DON'T KNOW	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO <input type="checkbox"/> DON'T KNOW

Total CM Performance Score =
 0=Poor...+11=Excellent

Total CM Plan Score =
 0=Poor...+11=Excellent

which subtype within a particular cluster is considered. What counts is that an organization has prepared for the possibility of at least one type occurring within each cluster.

Crisis-prepared organizations also prepare for at least one subtype in each of the main categories, because each type of crisis may be either the cause or the effect of another kind of crisis. For example, an economic downturn may set off a wave of criminal activities that in turn may make an industrial disaster more likely. Once again, it is important to take a systems point of view with regard to effective CM preparation. Like total quality management (TQM), CM is a systemic process. It does no good to prepare for only one type of crisis if another type can equally threaten or harm the organization.

CM-prepared organizations go even further. For instance, all organizations, not merely food and pharmaceutical companies, are subject to product tampering. The French publisher Larousse experienced a crisis that illustrates this point: As avid consumers of wild mushrooms, the French use the Larousse encyclopedia to differentiate between poisonous and edible mushrooms. On two pages, side by side, are pictures of mushrooms that are safe to

Figure 3.4. The eleven types of crises and their subtypes, continued.

eat opposite those that are not. For some unknown reason, the labels of the two pictures were reversed. Whether this was done by a careless editor or was an intentional, criminal act is not known and perhaps never will be.

The point is that every organization faces the possibility of some form of product tampering. For this reason, an integral part of the CM training and preparation process is brainstorming by the top members of an organization to consider how every category or type of crisis can apply to their organization. In order to come up with a broad spectrum of realistic examples, the members need to be prodded to think generally, not literally.

Phases

Figure 3.5 shows the five components of the factor *phases*: (1) signal detection, (2) preparation/prevention/probing, (3) damage containment, (4) business recovery, and (5) learning.

The first phase, *signal detection*, is the monitoring and heeding of early warning signals that point to the possible occurrence of a crisis. The explosion of the space shuttle *Challenger* is a prime example

Figure 3.5. The five components of the phases factor.

PHASES	Org Performed Well on the Factor in the Current Crisis?	Org Has CM CAPABILITY for the Particular Factor?
	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO <input type="checkbox"/> Don't Know	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> Don't Know
Signal Detection	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO <input type="checkbox"/> Don't Know	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> Don't Know
Preparation/Probing	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO <input type="checkbox"/> Don't Know	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> Don't Know
Damage Containment	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> Don't Know	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> Don't Know
Business Recovery	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> Don't Know	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> Don't Know
Learning	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> Don't Know	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO <input type="checkbox"/> Don't Know

****YES** = Org Did/Does Have a Particular Belief or Property
GIVE AN OVERALL Rating for Each Factor**

CM Performance Score = 3 0=Poor.....5=Excellent

CM Capability Score = 4

of a crisis whose early warning signals were ignored. The Report of the President's Commission on the Space Shuttle Accident uncovered a comprehensive trail of memos before the event clearly explaining that the O-ring was improperly designed and hence could cause a catastrophic failure of the shuttle.

The difficulty, of course, is that organizations are bombarded with signals of all kinds. However, it has been found that organizations that are crisis prepared make a point of constantly probing and scrutinizing their operations and management structure for warnings of potential crises. In other words, they do not leave the detection of important signals to chance. Instead, they put in place mechanisms to increase the chances of early detection.

The second phase, preparation/prevention/probing, is doing as much as possible to avoid crises and to prepare better for those that still manage to occur. This phase does not imply that all crises can be prevented; instead, it emphasizes that the adage "if it ain't broke, don't fix it" has no place in CM.

Those organizations that can be classified as crisis prone exhibit a very different "mind-set" from those that can be classified as crisis prepared. As in the case of signal detection, preparation/prevention/probing in crisis-prepared organizations is the careful and constant probing of operations and manage-

ment structures for potential "breaks and cracks" before they become too big to "fix." An example of a lack of attention to preparation/prevention/probing is Union Carbide's chemical explosion in its Bhopal, India, plant, during which thousands of people died because they had not previously been made aware of a basic safety response (i.e., covering one's nose and mouth with rags to avoid ingesting methyl isocyanate gas).

Damage containment is intended to keep a crisis from spreading to other, uncontaminated parts of an organization or its environment. A tragic example is the environmental costs of the Exxon Valdez oil spill, which were intensified by both poor damage containment mechanisms, such as inefficient oil-skimming equipment, and ineffectual damage containment activities, as well as the time lost in communicating among divisions of Exxon. A critical point regarding damage containment mechanisms and activities is that they are virtually impossible to invent during a crisis. Rather, effective CM requires the continued development and testing of CM capabilities before a crisis. In short, effective CM is proactive, not reactive.

During the recovery phase, crisis-prepared organizations implement short-term and long-term business recovery programs to facilitate the resumption of normal business operations. Programs designed for this purpose include the identification of minimal

services and procedures needed to resume business, the reassignment of people to new jobs, and the designation of alternative operating sites.

The last phase, learning, is the reflection on and examination of the lessons that have been learned from the organization's own crisis experiences, as well as those of other organizations. Many organizations gloss over this phase because of the mistaken belief that an examination of the past will "only reopen old wounds." But almost exactly the opposite has been found to be true. Following a crisis or near disaster, crisis-prepared organizations examine and compare the factors that enabled them to perform well with those that impeded their CM performance, without assigning blame. By contrast, crisis-prone organizations emphasize finding blame instead of learning lessons.

A valid CM audit assesses how well an organization is performing on each of these phases. (The scoring system used is a relatively simple one. Every yes that an organization gives to a particular component adds a one to its score. In comparison, the scoring system for the preceding variable types is much more complicated and is explained in Chapter 5.)

Figure 3.6 is based on Figure 3.5. It asks managers to evaluate in detail the damage containment strat-

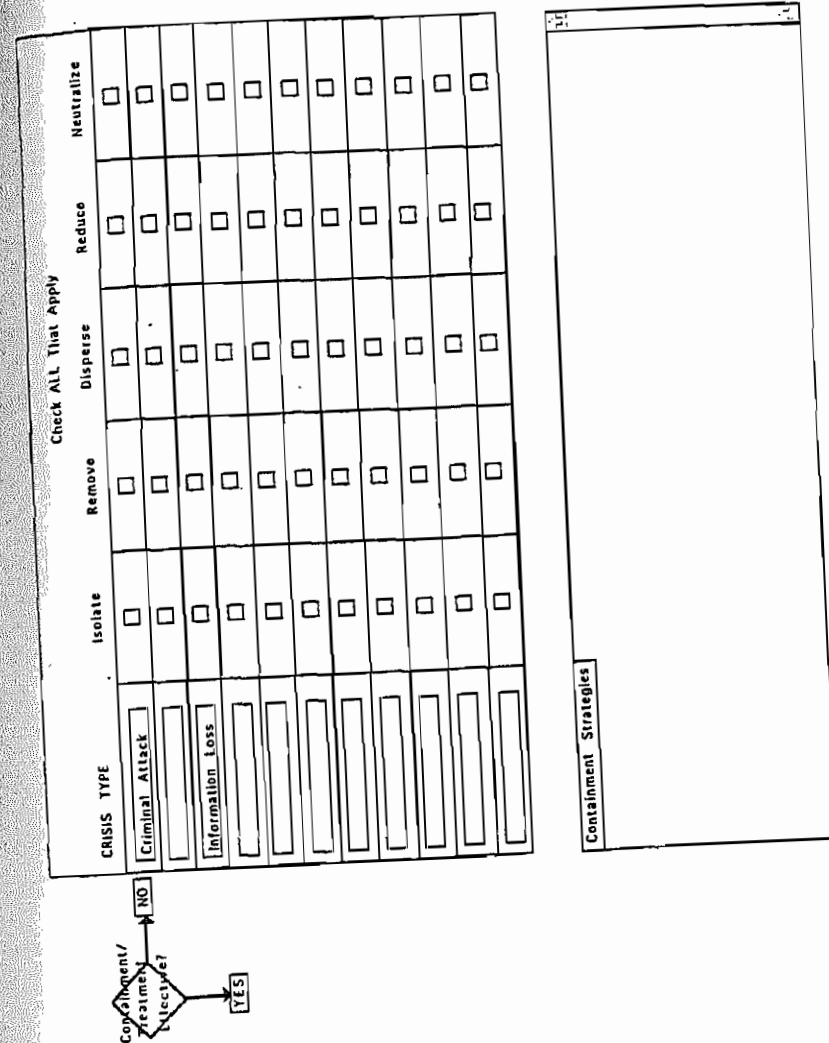


Figure 3.6. Damage containment strategies for each type of crisis.

egies for each type of crisis their organization faces. (Figure 3.6 also is part of the software package contained in the program CrMgt.)

Systems

Studies of a wide range of crises reveal that they occur because of breakdowns in the linkages among organizations, people, and technologies. No assessment of risk can be accurate unless it looks systematically at the interactions of all three subsystems. Unless an organization analyzes how (1) individual human operators and managers interact with technological systems, (2) people's limitations affect their reactions under stressful conditions, and (3) organizational factors (such as reward systems and communications channels) affect individual human responses, risk assessments will be incomplete at best.

CM plans and procedures need to specify the crisis roles and activities, lines of communication, membership on CM teams, backup resources, facilities, and schedules that people and systems in the organization must assume during a crisis. Just as important as documented plans and procedures is the effect of an organization's informal culture on its formal plans and procedures. One of the distinguishing hallmarks of crisis-prone organizations is a faulty mind-set or

belief structure. A study conducted by the University of Southern California Center for Crisis Management repeatedly found the same rationalizations that organizations used to explain why they thought they did not need to take CM seriously:³ "We're big enough to handle any crisis"; "Accidents are just the cost of doing business"; "CM is a luxury that we can't afford"; "If we have a major crisis, then someone else will rescue us." This study found that crisis-prone organizations subscribe to these beliefs seven times more than do crisis-prepared organizations.

Figure 3.7 is similar to Figure 3.5, except that each of the detailed attributes in each of the boxes has a negative connotation. Thus a "yes" response means that an organization does not have a particular defect. Also, to make the scoring easier and hence to reduce the amount of time spent going through the figures, the reader is asked merely to estimate an overall rating for each factor as a whole.

Stakeholders

Many parties are affected by and affect crises. *Stakeholders*—individual persons, special-interest groups, and institutions that affect or are affected by a specific organization—represent the diversity of views an organization should consider when formu-

	Org Performed Well on the Factor in the Current Crisis? <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> Don't Know	Org Has CM CAPABILITY for the Particular Factor? <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> Don't Know
SYSTEMIC FACTORS		
Org Infrastructure 1. Breakdown of Authority 2. Breakdown in Communication 3. Breakdown of CMT 4. Breakdown of Controls 5. Breakdown of Rewards 6. Breakdown of Reporting 7.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> Don't Know	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> Don't Know
Factors 1. Operator Errors 2. Faulty Maintenance 3. Faulty Man-Machine Design 4. Faulty Man-Org Interface 5. Faulty Systems Controls 6. Poor Training 7.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> Don't Know	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> Don't Know
Technology 1. Age of Equipment/Plants 2. Design Flaws 3. Faulty Maintenance 4. Severe Operating Conditions 5. Severe Operating History 6.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> Don't Know	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> Don't Know
Org Culture 1. Belief Can Handle Anything 2. Belief CM Not Worth the Money 3. Belief Org is Invulnerable 4. Denial of Need for CM 5. Denial of Magnitude of Threats 6. Denial of Possibility of Threats	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> Don't Know	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> Don't Know
Beliefs of TopMgt 1. Belief Can Handle Anything 2. Belief CM Not Worth the Money 3. Belief They Are Invulnerable 4. Denial of the Need for CM 5. Denial of Magnitude of Threats 6. Denial of Possibility of Threats	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO <input type="checkbox"/> Don't Know	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> Don't Know

YES = Org Performed Well by NOT Having the Particular Defect
 *YES** = Org Has CM Capability by NOT Having the Particular Defect
Give an OVERALL Rating for Each Factor

CM Performance Score = 4 CM Capability Score = 5

0 = Poor.....5 = Excellent

lating its CM plans and procedures. The current trend in management is to expand the number of relevant stakeholders beyond employees, managers, and unions to include customers and vendors. Effective CM requires an even greater expansion of relevant stakeholders to include parties even further removed from the organization, such as special-interest groups, local politicians, and even competitors. In sum, crisis-prepared organizations monitor and factor into their CM plans a much wider range of stakeholders than do crisis-prone organizations. For any organization, a systematic examination of diverse stakeholders and their associated properties is a critical part of the CM process. Figures 3.8 and 3.9 indicate the kinds of considerations that are necessary in the CM process with regard to major stakeholders, both internal and external. The questions on internal stakeholders focus on CMT membership, training, and access information.

DEVELOPING CM CAPABILITIES

The purpose of a CM audit is to identify an organization's major strengths and weaknesses so that a clear plan of action can be developed and imple-

Figure 3.7. The systemic factors of a crisis.

INTERNAL STAKEHOLDERS			
Officers	Positive Role In Current Crisis?	CMT Training?	Member of CMT?
	<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO
CEO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
COO	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
CFO	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
Legal	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
Security	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
PA	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
HR	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
Engineering	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
Health	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
Environment	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
	Crisis Performance Score: 4	CN Capability Score: 9	0 - Poor.....9 - Excellent
			LOCATION
			TELEPHONE #

mented to enhance its CM capabilities. Without such capabilities, an organization will find it very difficult to carry out the decisions and actions demanded in a crisis.

Figures 3.10 and 3.11 outline the main ingredients of a process intended to develop an organization's CM capabilities. The figures are essentially two different versions of the same thing. Both are intended to help an organization become CM prepared.

One of the first steps in developing an organization's CM capabilities is forming and training a CMT. The members of the CMT need to be selected with care and caution, and new members should not be added indiscriminately. A general rule is that a team should contain the smallest number of persons necessary to cope with a crisis. Most organizations' CMT has representatives from at least the following divisions: (1) Legal, (2) Security, (3) Human Resources, (4) Health and Safety, (5) Quality Assurance or Operations, and (6) Corporate Communications or Public Affairs. The organization's CEO should not automatically be made the leader of the CMT, although by the very definition of a crisis, the CEO and the top executives naturally need to have full information about the crisis and some degree of involvement.

Figure 3.8. CM considerations regarding internal stakeholders.

One of the most important roles of a CMT is that of a *facilitator*. The main functions of the facilitator are to make sure that all the team members have access to the same body of information and that no single point of view dominates the discussion.

THE ROLE OF SIMULATIONS IN CM

Simulations and training exercises are an essential part of the development of every organization's CM capabilities. A good simulation tests every aspect of the CM process described in this and the preceding chapter, including as many as possible of the dynamics represented in Figures 2.5, 2.7, and 2.9. (For instance, the types of crises represented in a simulation should test an organization's ability to respond simultaneously to multiple crises.) This means that the simulation should not be so transparent that the decisions and actions to be taken at every step are obvious or reduced to a single choice. Rather, a good simulation contains generous amounts of uncertainty. This forces the members of the CMT to state their assumptions as clearly as they can, reach agreement where they can, tolerate disagreement where they cannot, and identify at each step what they (1) know,

EXTERNAL STAKEHOLDERS				TELEPHONE #
STAKEHOLDER	Positive Role in Current Crisis?	ProCrisis Relationship?	History?	CONTACT
FBI	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input type="text"/>
STATE POLICE	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input type="text"/>
LOCAL POLICE	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input type="text"/>
FDA	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input type="text"/>
STATE HEALTH	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input type="text"/>
LOCAL HEALTH	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input type="text"/>
EPA	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input type="text"/>
STATE ENVIRONMENTAL	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input type="text"/>
LOCAL ENVIRONMENTAL	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	<input type="text"/>

Crisis Performance Score: 1-4 5-8 9-12 13-16 17-20

CM Capability Score: 1 2 3 4 5 6 7 8 9 10 11 12

Figure 3.9. CM considerations regarding external stakeholders.

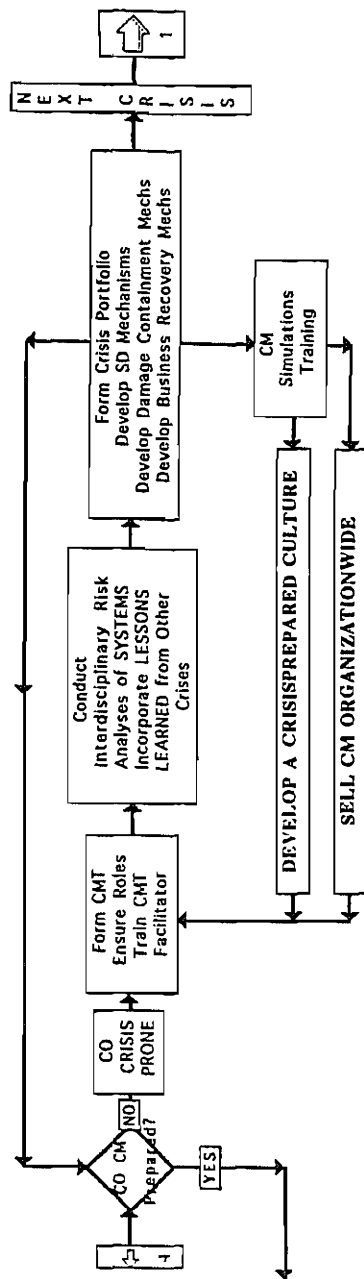


Figure 3.10. Development of CM capabilities.

(2) do not know, (3) must do immediately, (4) must postpone, and (5) must monitor and keep track of over time. The CMT also needs to keep track of both the details and the big picture of CM. An example of a simulation that we have constructed and used with organizations is given in Table 3.2.

As with all the various aspects of CM, we cannot emphasize too strongly that everything pertaining to an organization's CM capabilities and preparation should be tailored to its unique needs and circumstances. In CM, there are no useful "off-the-shelf" tools and procedures, and any person or group pretending to offer such aids should be rejected immediately.

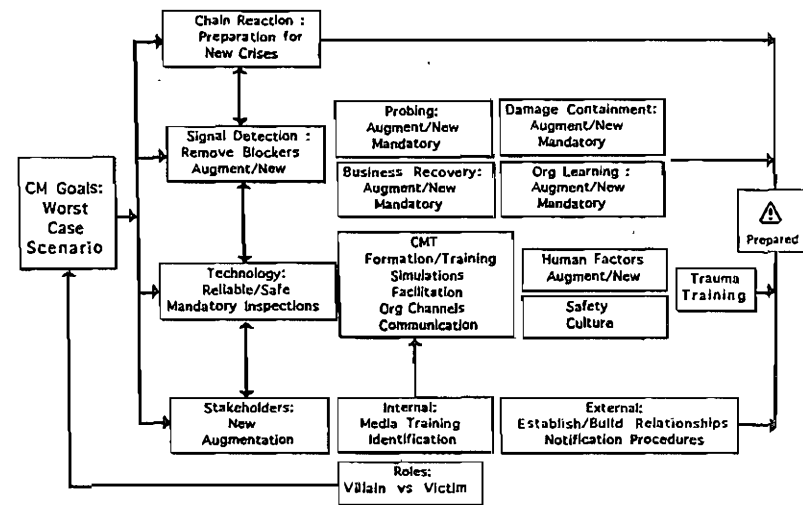


Figure 3.11. Development of CM capabilities, continued.

TABLE 3.2. HYPOTHETICAL CMT TABLETOP EXERCISE

Segment 1

MONDAY, 7:26 A.M.

As the Today Show fades to the local weather report, you catch just the tail end of Susan Jones's words: "This only substantiates the concerns we've expressed. We can't afford any more mishaps like Saturday's crisis at ChemCo's plant. I promise the fight is not over. As your attorney general, it is my duty to protect the people of this state."

Segment 2

MONDAY, 8:50 A.M.

Approximately thirty-six hours ago you should have received the first call regarding the serious fire and explosion at one of ChemCo's main plants, and now you may be facing the potential destruction of Blooming Gardens and the surrounding farmlands. There is also the possibility that a stretch of the Blue River could be contaminated by spills entering the sewers adjacent to the chemical plant. You can't help but think that something should have been done to prevent this disaster. Maybe if the incident had occurred when the superintendent was on duty, the damages could have been minimized.

Segment 3

MONDAY, 11:00 A.M.

An official from the state's Department of Natural Resources has phoned to inform you that they will be investigating any connection to ChemCo regarding the residents' complaints: Dead trout have been reported floating in the Blue River and Green Bay, with evidence of contamination by ChemCo.

Segment 4

MONDAY, 12:00 NOON

A status update confirms your worst suspicions. Toxic material leaking into drains has infiltrated the sewer system,

TABLE 3.2. (continued)

washing into the waste treatment plant. Projections indicate that all the flora and fauna of the treatment process may be killed by the leakage. How could the inspection conducted earlier this year have missed this problem? The engineers assure you that even though there were clear indications that pressure was building, measurements remained within established tolerance limits. Looking back, it all seems so obvious. If only a veteran operator had been taking the sample on Saturday. Surely someone who knew the system as well as his or her own car would have discovered the building pressure. Surely someone more experienced could have foreseen these problems.

Segment 5

MONDAY, 1:00 P.M.

A full picture of what is happening is beginning to emerge:

- 8:47 P.M., Saturday: The incident is first reported.
- 9:00 P.M., Saturday: Plant emergency response members are notified and go to the scene of the incident.
- 11:00 P.M., Saturday: The twenty-one injured people are taken to a hospital. The CMT is notified that four are confirmed dead and eight of the injured remain hospitalized.

Segment 6

MONDAY, 3:00 P.M.

CNN begins with a brief interview with a long-standing friend of ChemCo, Professor Frank Smith from Blossom State University. You're relieved that ChemCo is now getting some positive press, as Smith tells the interviewer, "ChemCo works to protect people and the environment as part of everything they do." You hope his statement may take some of the heat off your company. That makes two on your list of allies: The

(continued)

TABLE 3.2. HYPOTHETICAL CMT TABLETOP EXERCISE
(continued)

local union issued a statement earlier this morning assuring its members that it would continue to support ChemCo.

Two on your list of allies. And how many adversaries? Citizens for Environmental Advocacy has joined local environmentalist groups to express concern about the plant and the industry. You've had calls from competitors, with offers of assistance as well as criticisms of your presumed lack of attention to the facility. Some of ChemCo's national trade association representatives will be flying to the site later today. But your biggest surprise has been the media. Although the stories have certainly not been slanted in ChemCo's favor, the reporters have been willing to abide by your guidelines, and they have covered your briefings in a straightforward manner. If you could only convince them that ChemCo's intentions were earnest, that this site was a good and safe workplace.

Segment 7

MONDAY, 5:00 P.M.

Although there is some comfort that the site emergency response team performed well, you are concerned and angry that the area CMT was not notified more quickly. In addition, your thoughts are jolted once again. Your legal adviser reports that rumors of class-action suits are beginning to circulate.

Note: A group works on each time segment for approximately thirty minutes or less.

An Example

A recent crisis audit of a power utility that we performed illustrates its importance, especially in regard to what it can reveal about an organization. With regard to *types*, the audit clearly showed that in line with its business and mission, the utility was prepared mainly for natural disasters, especially those that would interrupt electrical service to its customers. Thus the organization had in place not only plans to deal with such disasters but also a day-to-day operational capability of responding to electrical and ice storms, fires, tornadoes, and other natural disasters. The utility was also rather well prepared for any threats to its equipment (the failure of electrical transformers) and technical systems in general.

In short, the utility was generally well prepared for technical crises, but it was not well prepared for large-scale systems accidents. For instance, it would not be prepared if five of its plants, located throughout its territory of operation, went out simultaneously. Most troubling, the audit revealed that the utility was not prepared for a broad range of human-induced crises such as sabotage or the kidnapping of an executive. It was certainly not prepared if a human crisis like sabotage led to a severe, large-scale technical crisis such as the shutdown of the entire system. This deficit was made even worse

by the fact that in general, security was lax at key locations.

The organization was especially deficient with regard to *phases*. For instance, not only were its signal detection mechanisms few and far between, but the audit disclosed that one of the most important sources of early warning signals was blocked rather effectively by the organization. It seems that maintenance personnel were in the best position to discover potential trouble spots. At the end of each shift, they filled out an evaluation form indicating the status of the machinery that they had inspected and/or on which they had performed maintenance. In theory, these forms were reviewed by their shift supervisors and passed on to their superiors. The trouble was that the status of the maintenance personnel was the lowest of any in the organization, and for this reason, their reports were generally ignored.

Notice that the low status of maintenance personnel affects not only the CM variable signal detection but systems and stakeholders as well. That is, the effects are systemic. The low status of the maintenance personnel compromises the detection of early warning signals and could also affect the safe operation of key equipment. In addition, this discovery also demonstrates the importance of analyzing the impact of a wide variety of stakeholders on an organization's crisis potential.

CONCLUDING REMARKS

Chapters 1, 2, and 3 introduced both the big picture and the details of CM, and they also covered what you need to consider and do before and after a crisis.

We believe that every organization should perform a crisis audit before it experiences a crisis. We also recommend that every organization perform at least one crisis audit a year and also after the occurrence of a crisis. Such audits are for the purpose of learning what patterns, if any, can be detected in an organization's responses, and they are invaluable in identifying crisis preparation strengths and weaknesses.

Notes

1. Thierry C. Pauchant and Ian I. Mitroff, *Transforming the Crisis Prone Organization* (San Francisco: Jossey-Bass, 1992). See also Ian I. Mitroff and Christine M. Pearson, *Crisis Management: A Diagnostic Guide for Improving Your Organization's Crisis Preparedness* (San Francisco: Jossey-Bass, 1993).
2. Ibid.
3. See Pauchant and Mitroff, *Transforming the Crisis Prone Organization*; see also Mitroff and Pearson, *Crisis Management*.