magnified for all to see, especially on the front pages of national newspapers and the opening minutes of national newscasts.

Notes

[1] Thierry C. Pauchant and Ian I. Mitroff, *Transforming the Crisis Prone Organization* (San Francisco: Jossey-Bass, 1992).

[2] Ibid.

[3] Ibid. See also Charles Perrow, *Normal Accidents: Living with High Risk Technologies* (New York: Basic Books, 1984).

[4] Quoted in Richard Behar, "Exxon Strikes Back," *Time*, March 26, 1990, p. 63.

[5] Peter Nulty, "Exxon's Problem: Not What You Think, the Embattled Oil Giant Is in Good Enough Financial Shape That It Can Almost Shrug off the Cost of the Alaskan Clean Up. But Morale and Long Term Leadership Are Another Matter," *Fortune*, April 23, 1990, p. 204.

[6] See Pauchant and Mitroff, *Transforming the Crisis Prone Organization*.

[7] For an in-depth discussion of systems and systems thinking, see Ian I. Mitroff and Harold Linstone, *The Unbounded Mind* (New York: Oxford University Press, 1993); see also Russell L. Ackoff, *The Democratic Organization, a Radical Prescription Recreating Corporate America and Rediscovering Success* (New York: Oxford University Press, 1994).

TWO

What to Do During a Crisis

A DETAILED GUIDE

Chapter 1 presented an overview of the actions that executives need to take during a crisis, the issues they need to address, and the relationship among these activities and issues. This relationship is important because in a crisis they need not only to attend to those issues requiring immediate attention but also to anticipate how their immediate actions will affect future actions. All the activities and decisions listed in Figure 1.1 are tightly intertwined and hence affect one another. For this reason, we believe that effective CM depends on how well an organization performs all the activities in Figure 1.1, and not on just one or two of them in isolation.

In this chapter, we will explore in more detail each of the boxes in Figure 1.1. To do this, we will use other figures that seem different from Figure 1.1. As before, we will both examine the activities and decisions one at a time and show them in relationship to one another so that as you are performing one activity, you can plan for those following it.

THE INITIAL INFORMATION AND ACTION PHASE OF CM

The First Point of Contact: The Accuracy, Credibility, and Power of the Initial Sources of Information

Figure 2.1 illustrates the beginning phase of CM, how a crisis comes to an organization's attention. Box 1 of this figure indicates that a crisis can be brought to an organization's attention by either internal or external sources or some combination of the two.

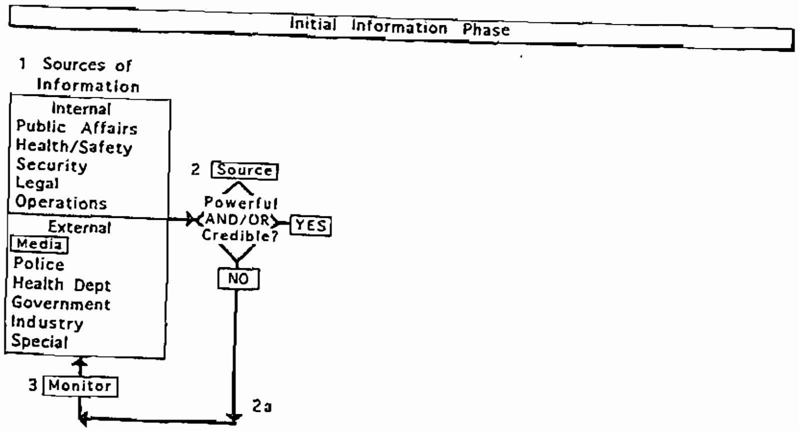


Figure 2.1. The first decision: finding out how a crisis comes to an organization's attention.

The first critical decision that every organization must make pertains to the power and/or credibility of the source bringing the crisis to its attention. (In all the following figures, a critical decision is enclosed in a diamond, and the outcomes of decisions or activities are in rectangles.) If the source is judged to be neither powerful nor credible (the "no" box just below Diamond 2 in Figure 2.1), the organization is advised to monitor (Point 3) the situation carefully in order to determine whether the initial information is an early warning signal of an impending crisis.

Determining the power and credibility of an information source is obviously a judgment call, as are most of the decisions required in CM, and so they depend on the experience, knowledge, and skills of the person or persons monitoring the incoming information. This does not mean that there are no sound bases on which to make the initial decisions with regard to a source's power and/or credibility. Indeed, such judgments are likely to be based on the experience and expertise of relevant members of the organization. For example, a call from *60 Minutes* or *Nightline* should be considered important (i.e., powerful), no matter what its credibility. By definition, inquiries from any major national publication should also be taken very seriously. The point is that the initial phase of CM invariably involves judgments with regard to the potential seriousness of a situation.

Since the notion of "power" is essential here, we should say a bit more about its definition. An example of the traditional definition of power is that person A is said to have power over person B if A can force B to perform actions that on his or her own, B would not perform. More generally, A is said to have power over B if A can "influence" B's behavior. This definition applies to CM as well, but another, more important definition also applies: One person or, more generally, one stakeholder, A, has power over another stakeholder, B, if A can cause a noncrisis situation to become a crisis for B. According to this definition, the news media certainly have power, and therefore a call from a representative of a major news organization should be taken very seriously. Indeed, the call itself should be regarded as a "potential crisis," and not merely an "incoming message."

On the other hand, a call or action by one of the major news media does not mean that an organization should automatically admit guilt. In some cases, it should contest allegations of wrongdoing. A classic example is NBC's showing GM trucks catching fire: GM successfully contested the charges and proved that NBC had deliberately tampered with GM's products to produce the story. As with the earlier definition of power, we can say that one expert, A, is more credible than another, B, if A can force an organization into a crisis situation.

To Be or Not to Be Proactive

If a source is deemed to be powerful and/or credible, the next critical decision an organization faces is whether or not it should be "proactive." Should the organization move into an active crisis response mode *before* the full extent of damage or injuries (if any) can be established? In many cases, regardless of whether or not the organization is responsible for any damage or injuries, being proactive can be a real plus. That is, the organization will have acted responsibly on its own without being prodded by other forces or agencies. The risk, of course, is that quick actions may not only be ill conceived but also may imply guilt. In some cases, quick actions may also cost an organization sizable amounts of money or other resources. Yet in many cases, organizations report winning generous amounts of goodwill for their early actions.

Once an organization decides to be proactive, the next critical decision (Figure 2.2, Point 5) is whether it is prepared for CM. The decision in this case is not whether the organization "determines" at this time that it is prepared to handle a crisis but whether the actions it has taken in the past have prepared it to handle a crisis.

If the organization is proactive (Point 4a) and is prepared for CM, its first action should be to activate its crisis management team (CMT) (Point 6). On

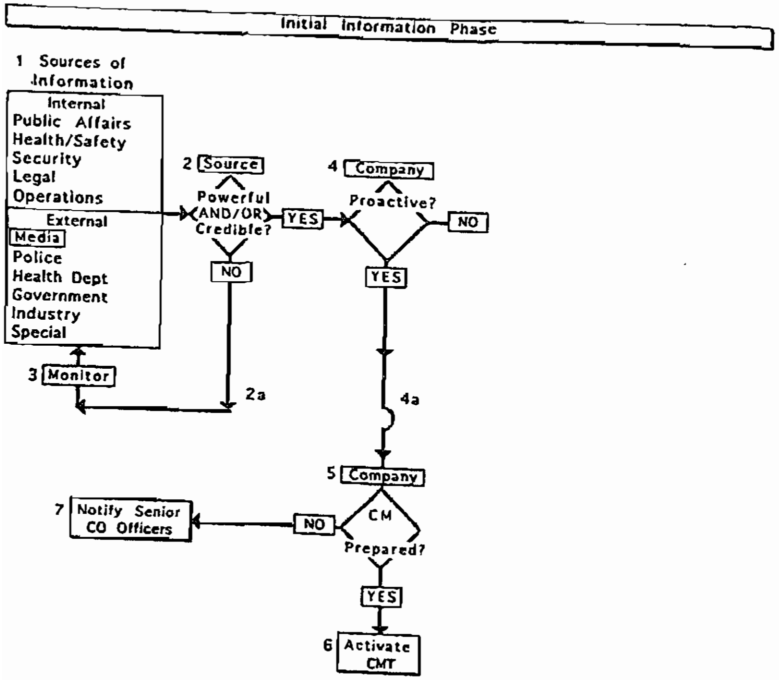


Figure 2.2. The second decision: whether an organization is prepared for CM.

the other hand, if the organization is not prepared for CM, each of its senior officers (Point 7) must be notified immediately.

There is a vicious paradox associated with not being prepared: If an organization is ill prepared, then it is unlikely that its senior officers will be notified in a timely fashion, if at all. One of the noticeable characteristics of organizations that are not well prepared is that they do not convey important information from one part of the organization to others, for reasons that we shall examine in more detail later.[1]

To Assume or Not to Assume Responsibility?

Figure 2.3 shows the next series of critical CM activities and decisions. One characteristic of CM-prepared organizations (the "yes" box preceding Point 6) is that they are ready to assume responsibility for a crisis before they know all the particulars of the case at hand (e.g., the full extent of injuries and whether or not the organization is responsible for them). As a general rule, CM-prepared organizations assume responsibility (Point 9) even when they are not responsible.[2] This does not mean that they are pushovers that accept responsibility for everything (Point 8); rather, it means that concern for their consumers, employees, the general public, and the environment is valued over immediate, short-term profits. (Johnson & Johnson's handling of the Tylenol poisonings is an excellent example of this kind of behavior.[3])

CM-prepared organizations understand implicitly that concern for people and the environment is vital to their continued existence and hence to their long-term profits. For this reason, at the very first sign of a crisis, they commence a coordinated crisis response

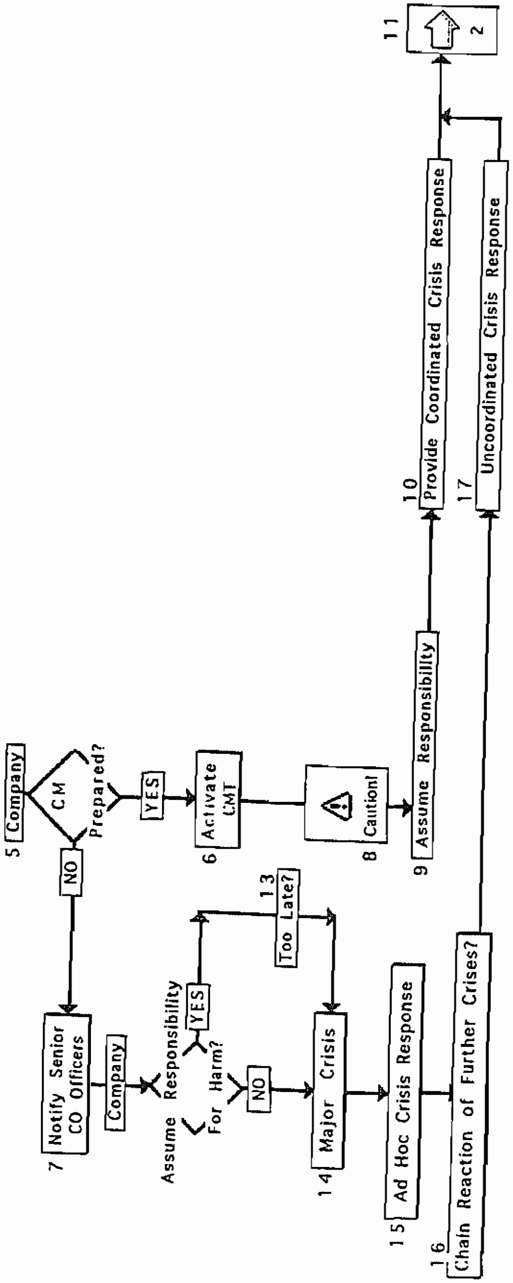

5 Company
CM Prepared?
YES
NO
6 Activate CMT
8 Caution!
9 Assume Responsibility
10 Provide Coordinated Crisis Response
11
2
7 Notify Senior CO Officers
Company
Assume Responsibility For Harm?
YES
NO
13 Too Late?
14 Major Crisis
15 Ad Hoc Crisis Response
16 Chain Reaction of Further Crises?
17 Uncoordinated Crisis Response

Figure 2.3. The third decision: whether an organization is prepared to assume responsibility for a crisis.

(Point 10). As soon as possible, a member of their CMT is sent to the site of the crisis to begin fact-finding and to coordinate recovery and treatment activities. CM-prepared organizations also are able to enhance their response by mobilizing their crisis command centers. They call important external stakeholders such as government agencies, research contract labs, and other firms that can provide specialized CM expertise. Such organizations have developed and tested all the relevant contacts far in advance so that they do not have to scramble to make those contacts during a crisis.

Figure 2.3 also shows the kind of scrambling required by a CM-unprepared organization. Even if it assumes responsibility for harm (Point 13), it may be delayed or too late. If the organization has caused harm and does not assume responsibility (Point 14), then its lack of preparation will become part of the crisis itself (Point 15), as it will compound its errors (Point 16) by virtue of its ad hoc and uncoordinated crisis responses (Point 17). All this will result in a chain reaction of further crises (Point 16) that bring additional uncoordinated crisis responses (Point 17).

Seriousness and Responsibility

Figure 2.4 shows the series of decisions and activities that will be needed if an organization decides not

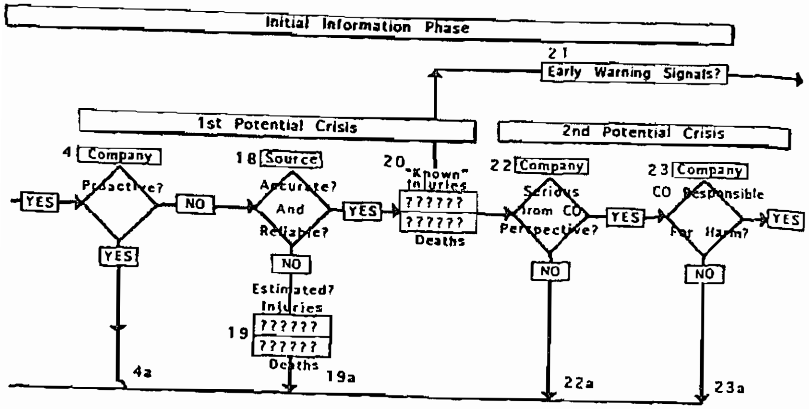


Figure 2.4. The fourth decision: determining the seriousness of a crisis and the organization's responsibility for it.

to be proactive (the "no" decision box to the immediate right of Diamond 4; see also Figure 2.2). In this case, the decision to act is deferred until more accurate and reliable numbers are collected regarding the extent and seriousness of injuries (Point 22). If the available numbers are deemed inaccurate and unreliable (Point 19a), the situation should be monitored for further developments (Figure 2.1, Point 3). If the numbers are believed to be reasonably accurate and reliable and hence "known" (Point 20), questions (Points 22 and 23) should be asked about (1) the seriousness of the crisis from the company's point of view and (2) whether or not the company is responsible for the crisis.

Note that in reality, there are far too many decision loops to show each of them here. For instance, even if the available numbers (Diamond 18) are not deemed accurate or reliable, the organization may still decide to proceed (Diamond 22) because it feels the situation may be important and so may decide to dispatch a member of its CMT, or another top executive, to examine the situation more closely.

The determinations of seriousness and responsibility naturally raise the important issue of what the criteria are that should influence an organization to accept responsibility and act. Although there is no one answer to this problem, we can offer some guidelines. Table 2.1 shows the criteria used by two very different organizations with whom we have worked that should trigger a crisis response. The left-hand column pertains to a company in the chemical industry, and the right-hand one, to one in the food industry.

In effect, the criteria constitute a threshold. If an event meets or exceeds any of the criteria listed in each row of the table, the company should act decisively. Note that although there are distinct differences between the two sets, there is nonetheless a remarkable degree of overlap between them. The criteria are thus broadly applicable to organizations no matter what their business.

TABLE 2.1. CRITERIA/EVENTS THAT WILL TRIGGER A CRISIS RESPONSE

Industrial Crisis	Food-Related Crisis	Your Organization
1. Affects the outside community or environment: The incident closes major major roads or public facilities.	1. One serious consumer injury.	1.__________ __________ __________ __________
2. Causes fatalities (one or more).	2. Two complaints of illness or injury with regard to the same product/code.	2.__________ __________
3. Causes multiple injuries or exposure to a serious chemical hazard.	3. Likelihood of recall or withdrawal.	3.__________ __________
4. Releases known carcinogens or toxic materials even if they are contained in a sealed-off area.	4. Media or agency involvement.	4.__________ __________ __________ __________
5. Draws media attention from the outside.	5. Tampering or a threat of tampering.	5.__________
6. Enters a waterway.	6. Serious injury involving facility or employees.	6.__________
7. Forces a master shutdown or complete evacuation of facilities, thereby attracting media attention.	7. Facility explosion or fire.	7.__________ __________ __________

TABLE 2.1. (continued)

Industrial Crisis	Food-Related Crisis	Your Organization
8. Is of sufficient magnitude to require regulatory notification.	8. Bomb threat, kidnapping.	8.__________ __________
9. Shuts down an operating unit.	9. Facility evacuation.	9.__________
10. Is a repetition of similar events.	10. Spill or leak.	10.__________
11. Has an extended duration of more than five hours.	11. Serious property damage to facility caused by weather or violence.	11.__________ __________
12. Is any special circumstance that might escalate the event/issue.	12. Strike/walkout at facility.	12.__________ __________
	13. Health/safety problems at facility.	13.__________
	14. Civil unrest near facility.	14.__________
	15. Media attention.	15.__________

Delayed Response

Figure 2.5 shows the full set and sequence of critical decisions and activities that comprise the initial information-gathering and action phases of CM. It shows that the precipitating crisis can lead to several more crises (the first, second, third, and fourth potential crisis phases), depending on how the organization responds or is perceived to respond. Figure 2.5 shows that if the response to the initial crisis is delayed too long in order to collect sufficiently accurate and reliable numbers (Point 24) and if the company is not prepared for CM, the delay itself can further fuel the initial crisis (Point 13).

One of the most important lessons to be learned from the way in which crises unfold is that every organization needs to formulate criteria for action that are specially suited to its situation. The criteria are essential to helping determine which direction to move in as the organization proceeds through Figure 2.5. Of course, we can offer only general guidelines for your organization to consider.

Figure 2.5 shows the kinds of issues you should consider during a crisis and also, ideally, before one occurs. After you have studied the figure, you can begin to appreciate why CM requires preparation

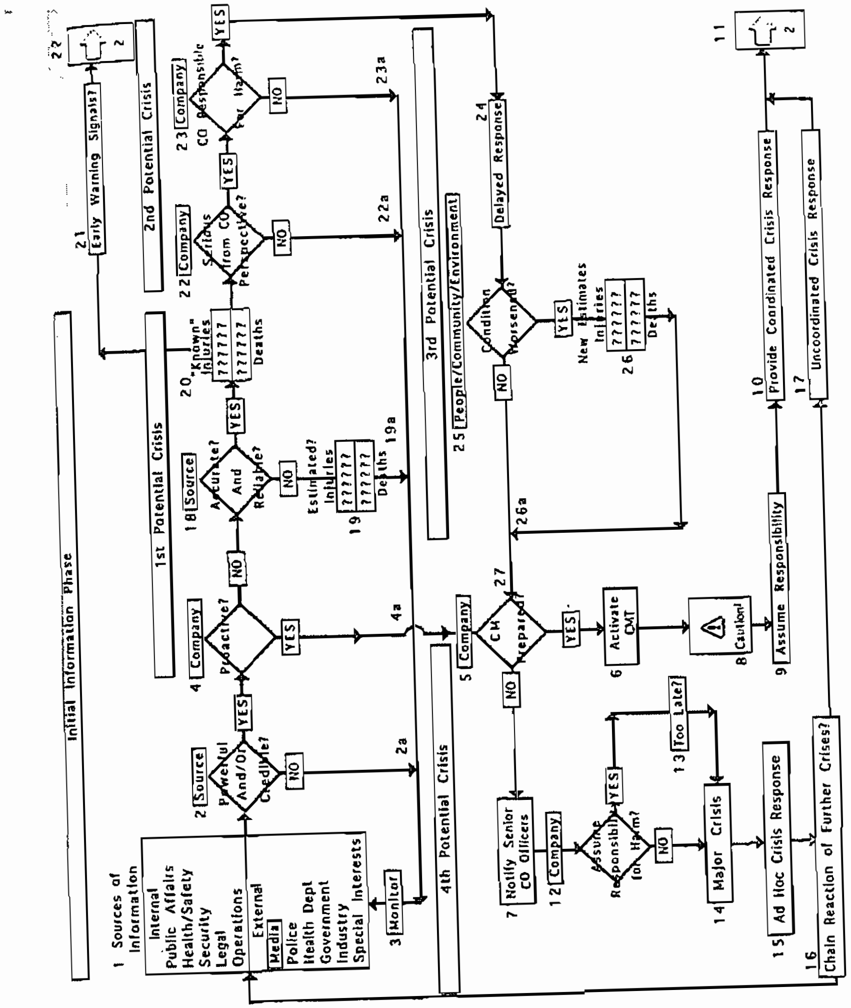


Figure 2.5. The fifth decision: making the initial information-gathering and action decisions.

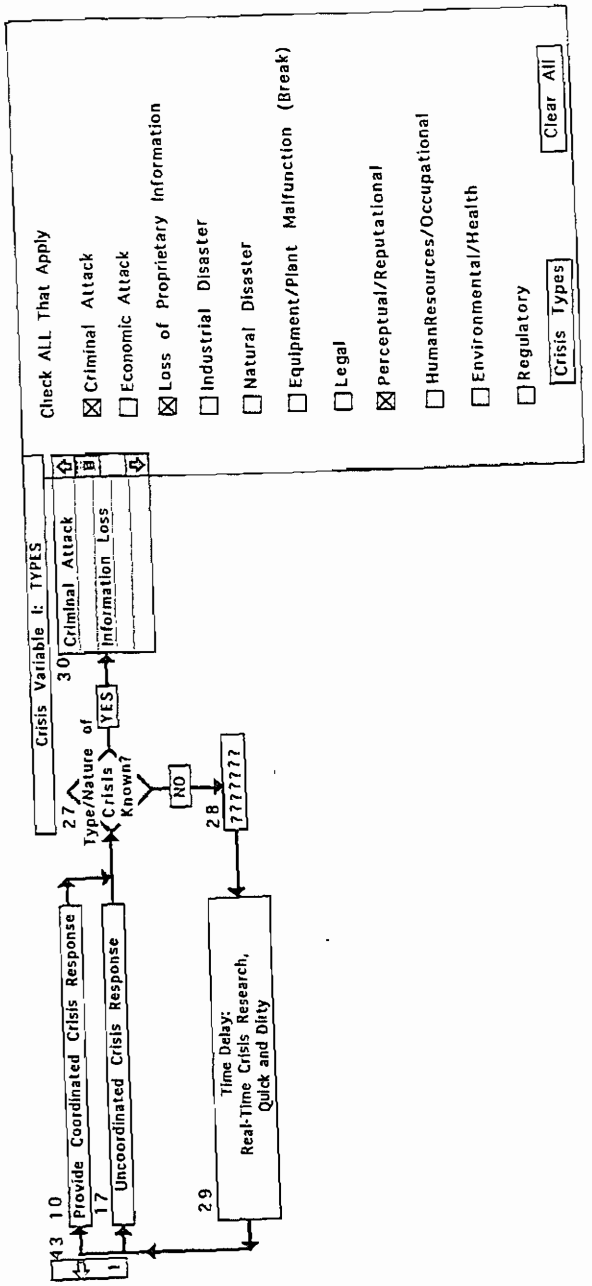
before a crisis. There are too many issues and activities occurring throughout the process of Figure 2.5 to "ad hoc it." Unprepared companies can expect some dissension and infighting, which only will intensify the crisis. This may be true even of those organizations that are somewhat CM prepared, since every crisis unleashes powerful emotions.[4] Typically, in unprepared organizations, untrained senior officers can be expected to retreat to their specialized training and their usual ways of reacting to stress.

DIAGNOSING THE CRISIS

What Is the Crisis?

Figure 2.6 shows the next series of critical activities and decisions making up the second major part of the CM process. Despite whether an organization is prepared for CM (Figure 2.5, Point 6) or not (Figure 2.5, Point 27), and hence executes a coordinated or uncoordinated crisis response, the precise type and nature of the crisis must be determined.

There are eleven basic types of crises, ranging from criminal attacks to punitive regulatory legislation. (We will examine the various subtypes of these eleven basic types in more detail later.) In addition, though they are distinct, these basic types are neither exhaustive nor exclusive. Because of its complexity,


43
10 Provide Coordinated Crisis Response
17 Uncoordinated Crisis Response
27 Type/Nature of Crisis Known?
YES
NO
28 ???????
29 Time Delay: Real-Time Crisis Research, Quick and Dirty
30 Crisis Variable I: TYPES
Criminal Attack
Information Loss
Crisis Types
Clear All

Check ALL That Apply

☒ Criminal Attack
□ Economic Attack
☒ Loss of Proprietary Information
□ Industrial Disaster
□ Natural Disaster
□ Equipment/Plant Malfunction (Break)
□ Legal
☒ Perceptual/Reputational
□ HumanResources/Occupational
□ Environmental/Health
□ Regulatory

Figure 2.6. The sixth decision: determining the type of crisis.

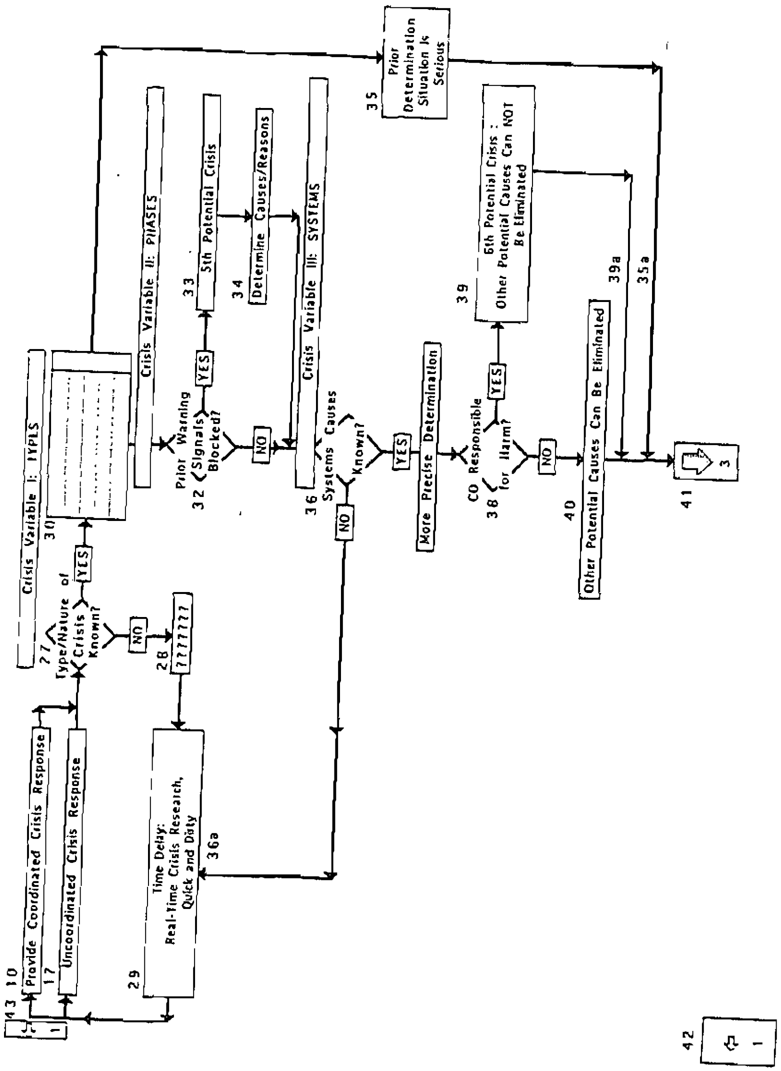

Crisis Variable I: TYPES
30
Crisis Variable II: PHASES
33
5th Potential Crisis
34
Determine Causes/Reasons
Crisis Variable III: SYSTEMS
35
Prior Determination Situation Is Serious
39
6th Potential Crisis: Other Potential Causes Can NOT Be Eliminated
39a
35a
More Precise Determination
40
Other Potential Causes Can Be Eliminated
41
3
42
1
32
Prior Warning Signals Blocked?
YES
NO
36
Systems Causes Known?
YES
NO
38
CO Responsible for Harm?
YES
NO
27
Type/Nature of Crisis Known?
YES
NO
28
???????
29
Time Delay: Real-Time Crisis Research, Quick and Dirty
36a
43
10
Provide Coordinated Crisis Response
17
Uncoordinated Crisis Response
1

Figure 2.7. The seventh decision: deciding on an organization's CM preparation and response.

a crisis may fall into one or more types at the same time, depending on the circumstances, and any one of the types in Figure 2.6 is capable of causing any other type. That is, any of the types can be the cause and/or the effect of any other.[5]

A crisis's precise nature or type may not always be immediately apparent, which is one of the best reasons for not taking immediate or drastic action until the nature and extent of injuries have been determined (Figure 2.5, Point 20). Moreover, if your organization is crisis prepared, when you begin determining the numbers of injuries, you should also begin determining the type of crisis that produced the injuries. In other words, identifying a crisis and determining whether injuries have resulted are complementary acts; they should not be viewed as separate activities. This is a strong justification for considering the set of crisis activities and decisions as an integrated whole. When you take a particular action or decision, you should be thinking how it will influence others.

Figure 2.8 shows that if you do not know (as indicated by the giant question marks) the "type" of a crisis (Figure 2.7, Point 28), you will lose time (Point 29) finding out. The activities in Figure 2.7, Box 29,

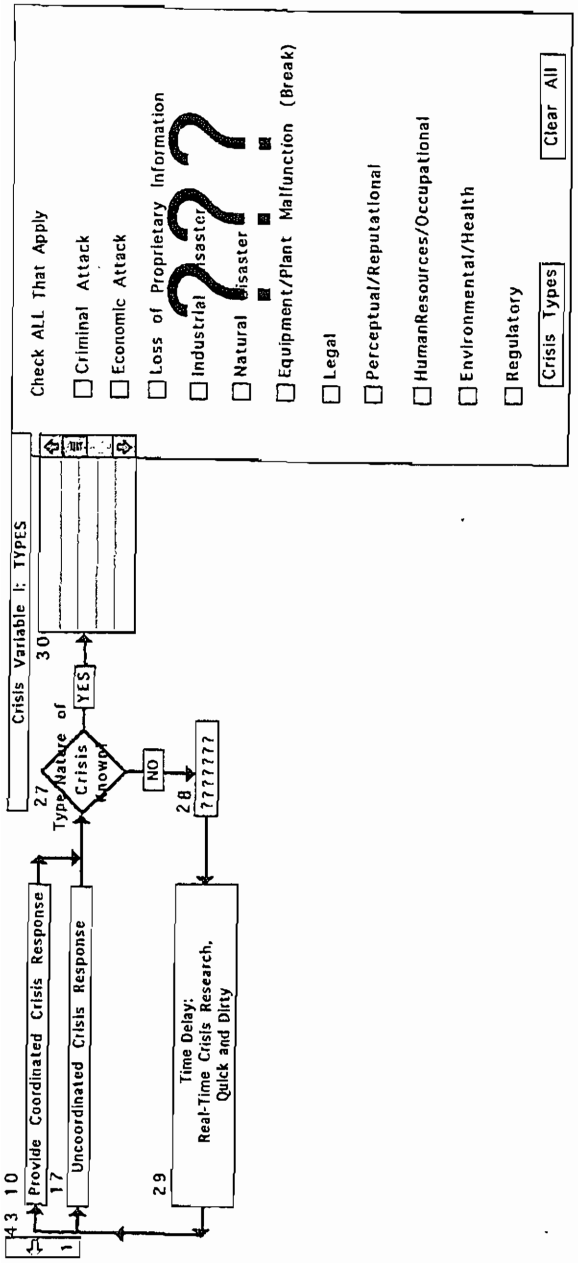

Crisis Variable I: TYPES
30
27
Type/Nature of Crisis Known?
YES
NO
28
???????
29
Time Delay:
Real-Time Crisis Research,
Quick and Dirty
43 10
Provide Coordinated Crisis Response
17
Uncoordinated Crisis Response
1
Check ALL That Apply
□ Criminal Attack
□ Economic Attack
□ Loss of Proprietary Information
□ Industrial Disaster
□ Natural Disaster
□ Equipment/Plant Malfunction (Break)
□ Legal
□ Perceptual/Reputational
□ HumanResources/Occupational
□ Environmental/Health
□ Regulatory
Crisis Types
Clear All
???

Figure 2.8. Why not being prepared loses time.

are critical because further actions and decisions presuppose some knowledge, however sketchy, of the crisis's type.

Point 32 in Figure 2.7 asks whether any early warning signals associated with the crisis were blocked or not transmitted in the appropriate language to the appropriate person at the appropriate place and time in the organization. One of the most important findings in CM is that with very few exceptions, crises send out a trail of early warning signals before their actual occurrence.[6] If such signals can be detected, many crises can be prevented from occurring—the best possible form of CM. If the signals associated with a crisis were blocked, then finding out what the particular kinds of blocks were can help prevent future crises. But once a crisis has occurred and an organization is under the magnifying lens of the media, there can be few secrets. Indeed, it is likely that the fact that early warning signals were blocked will be revealed, and so become part of the crisis itself. For this reason, it is important to know whether any early warning signs were present and how they were handled. For instance, one of the biggest contributing factors to the explosion of the *Challenger* was the fact that messages warning of the potentially unsafe condition of the O-rings were prevented from reaching those at the top of NASA's hierarchy.[7]

In a similar manner, those activites occurring in Crisis Variable III, SYSTEMS (Figure 2.7, Point 36) encompass a whole set of investigative actions designed to uncover the causes of a crisis. If the causes are not known (Point 36a), a "quick and dirty" investigation to determine the crisis's causes will be necessary.

The following factors have been shown to be present in every crisis: (1) technology, (2) human factors, (3) organizational structure, (4) culture, and (5) top management psychology. Most organizations have core technologies that are closely linked to the production of their key products and services. For instance, certain chemical processes constitute the core technology of a chemical refinery. Computers are one of the most vulnerable technologies of virtually every organization.

A second cause of organizational crises is "human factors." All technologies are operated by people who cannot be presumed to be infallible. Operators often make errors, with job overload and stress increasing that probability. Thus, the possible human causes of every crisis must be examined.

If technologies could exist and operate on their own, we might not have crises; unfortunately, however, technologies and people are interdependent. Power, authority, and egos often get in the way of safe operations when organizations conceal vital information. A recurring question in trying to determine the cause of a crisis is whether an organization's channels of communication have been blocked. If so, how did this contribute to the crisis? Did the organization's reward system contribute as well? For instance, is getting products out the door valued more highly than safety? These are only a few of the questions to ask about the potential contributions of organizational factors to crises.

An organization's culture has also been found to be a principal cause of many crises. Indeed, certain organizations are labeled *crisis prone*.[8] Such organizations embody attitudes that almost guarantee a crisis. That is, they use rationalizations (e.g., "We're so big and powerful that nothing bad can happen to us") to deny their need for advanced CM planning and preparation. At the other extreme, a much smaller number of organizations are *crisis prepared*.

Finally, the attitudes and values of top executives have been found to be strong contributing factors. If an organization's managers believe that they and their organizations are invulnerable, a crisis is much more likely.

All these factors (Figure 2.7, Point 38) affect whether or not an organization is responsible for harm. Only when all other factors or explanations can be eliminated (Point 40) can we say for sure that the organization was or was not responsible. The facts uncovered by the investigations (Points 32, 36, and 38) are thus critical, as they determine subsequent actions to (1) contain the crisis, (2) treat it, (3) communicate to the authorities and other important stakeholders, and (4) learn from the crisis.

TREATING THE CRISIS

Containment and Treatment

Figure 2.9 shows why knowing the particular type of a crisis and its specific causes is important. When you do not have such knowledge, it is very difficult to contain the crisis and treat its full effects, and you do not know which containment and treatment options are best.

The five basic types of containment and treatment options are (1) isolation, (2) removal, (3) dispersal, (4) reduction, and (5) neutralization. First, for isolation, we physically or psychologically separate—or attempt to separate—the crisis from the organization. For instance, in the case of a toxic or hazardous spill, we put a physical barrier around the spill area to contain and isolate it from the rest of an organization or community. In the case of a political or

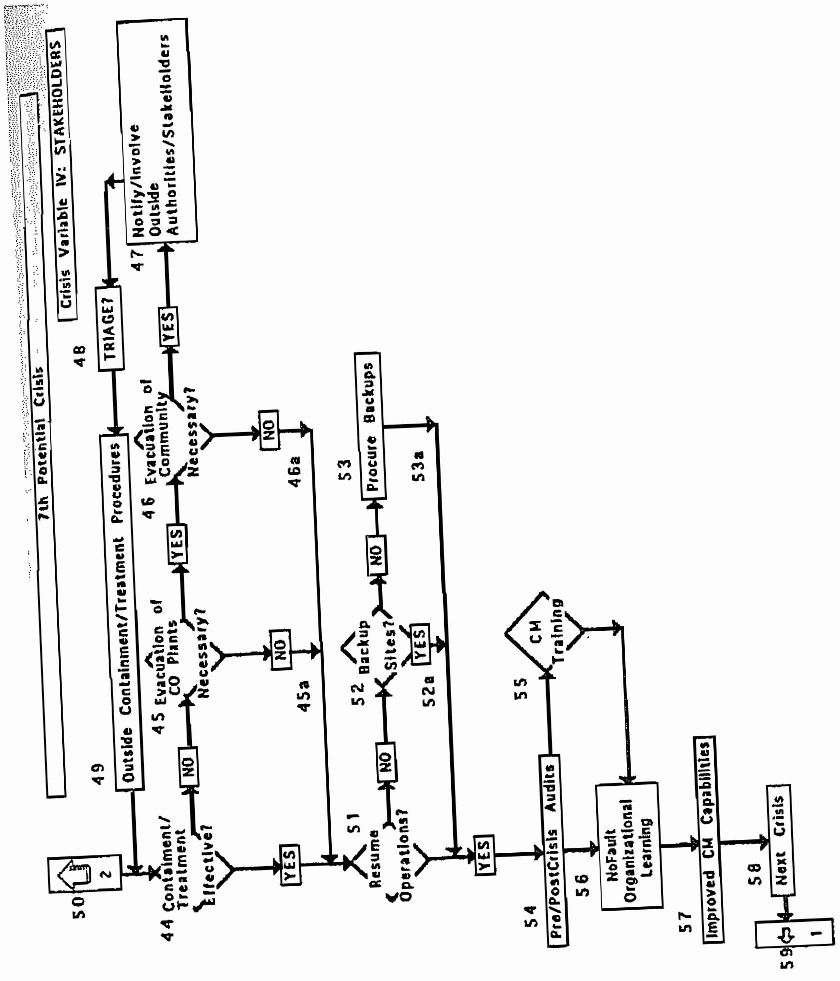

7th Potential Crisis
Crisis Variable IV: STAKEHOLDERS
48
TRIAGE?
47
Notify/Involve Outside Authorities/Stakeholders
49
Outside Containment/Treatment Procedures
46
Evacuation of Community Necessary?
YES
YES
NO
46a
45
Evacuation of CO Plants Necessary?
NO
NO
45a
44
Containment/Treatment Effective?
YES
50
2
51
Resume Operations?
NO
YES
52
Backup Sites?
NO
YES
52a
53
Procure Backups
53a
54
Pre/PostCrisis Audits
55
CM Training
56
NoFault Organizational Learning
57
Improved CM Capabilities
58
Next Crisis
59
1

Figure 2.9. The eighth decision: deciding on containment and treatment.

reputational crisis, we contain it by attempting to isolate it psychologically (i.e., in the minds of people), by differentiating it from the rest of the organization or a particular person.

For the second option, removal, we attempt to remove physically a crisis or its effects, for example, when we physically remove a toxic spill from a particular location. If we cannot physically remove a crisis or its effects, we should try to disperse it or its effects, reduce it, or neutralize its potency.

To Evacuate or Not to Evacuate?

If containment and treatment are not sufficient (Figure 2.9, Point 44), we should decide whether the physical evacuation of an organization's facilities or its surrounding community is necessary. Note that the term *evacuation* is not meant literally. For instance, you may be faced with having to abandon or discontinue a product or even a business unit of an organization, because the damage to a particular brand, factory, plant, or product is so severe that it must be jettisoned in order to save the rest of the organization. As with everything else, evacuation cannot be considered in isolation. Outside authorities such as the public health authorities and the police probably should be notified (Figure 2.9, Box 47), if only to coordinate the community's response and

evacuation. In some cases, the crisis may be so serious that a triage of employees and the surrounding communities must be undertaken. Finally, if the organization is unable to contain the crisis completely on its own, outsiders should be brought in (box 49).

Business Resumption

Once a crisis is brought under control and its effects have been contained or mitigated to the point that they no longer constitute a threat to the organization or its external stakeholders, the resumption of business is the next step (Figure 2.9, Diamond 51). If you cannot resume full operations at an organization's sites, are backup sites available (Diamond 52)? If they are not available, temporary facilities may have to be found. You may want to resume certain operations as soon as possible to indicate to key customers that the organization is still in business and hence is both able and willing to serve them. Any temporary backup sites should also provide for the maintenance and storage of critical information, computers, and telecommunications. This includes both "hot" and "cold" storage sites. *Hot* sites enable an almost instantaneous switchover to backup databases, computers, and telephones in the event of a shutdown. This includes securing alternative trunk or communication lines from telephone companies. *Cold* sites, on the other hand, refer to the regular backup of key records in protected, off-site storage facilities, without immediate access to backup equipment.

A critical factor in backing up plants, facilities, information, telecommunications, and the like is that backup operations must be considered as a whole. It is no longer sufficient to back up individual sites, work stations, facilities, or pieces of equipment, since entire systems can now fail because of the complexity and the interconnectedness of technology.

Finally, backup activities require an organization to identify those of its key customers who need to be serviced quickly or continuously and on whom the organization depends for its operations. Likewise, you should find out who the critical vendors or suppliers of goods and services are on whom the organization depends in order to serve its key customers.

CONCLUDING REMARKS

For those readers interested in seeing how Figures 2.5, 2.7, and 2.9 relate to one another and also fit into the overall process of CM, Figure 2.10 is available; it shows the entire CM process. (Readers can obtain a copy of Figure 2.10 by mailing in the card included with this book.)

By now, it should be apparent why effective CM during a crisis requires effective preparation before it occurs. Most of the key decisions and activities that must be considered and undertaken during a crisis cannot be performed effectively if you or your organization lack the proper preparation and CM capabilities. Accordingly, we turn next to the activities you should perform before and after a crisis.

Notes

1. Ian I. Mitroff and Thierry C. Pauchant, *We're So Big and Powerful Nothing Bad Can Happen to Us: An Investigation of America's Crisis-Prone Corporations* (New York: Birch Lane Press, 1990).
2. Ibid.
3. See Ian I. Mitroff and Ralph H. Kilmann, *Corporate Tragedies, Product Tampering, Sabotage, and Other Catastrophes* (New York: Praeger, 1984).
4. Mitroff and Pauchant, *We're So Big and Powerful.*
5. Thierry C. Pauchant and Ian I. Mitroff, *Transforming the Crisis Prone Organization* (San Francisco: Jossey-Bass, 1992).
6. Ibid.
7. Ibid.
8. Ibid. See also Christine M. Pearson and Ian I. Mitroff, "From Crisis Prone to Crisis Prepared: A Framework for Crisis Management," *Academy of Management Executive* 7 (1993): 48–59.