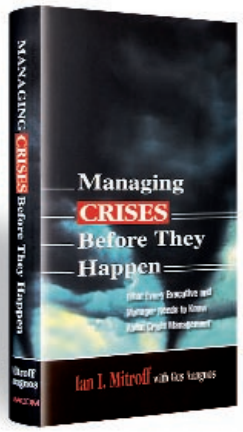
SOUNDVIEW Executive Book Summaries®



What Every Executive Needs to Know About Crisis Management

MANAGING CRISES BEFORE THEY HAPPEN

By Ian I. Mitroff with Gus Anagnos

CONTENTS

The Five Components of a Crisis Management Framework
Page 2

Types and Risk Categories of Crises
Pages 2, 3, 4

Mechanisms to Prepare for and Respond to Crises
Pages 4, 5

Organizational Systems
Pages 5, 6

Don't Forget Your Stakeholders
Page 6

You Are Now Ready to Develop Crisis Management Scenarios
Page 7

How Telling the Truth Is Vital to Crisis Management
Page 7

Assume Responsibility Or Pay the Price
Page 8

Crisis Management: An Exercise in Creative Thinking
Page 8

THE SUMMARY IN BRIEF

While emergency and risk management deal with natural disasters, crisis management is concerned with human-caused disasters — a permanent and prominent feature of today's societies. A sample includes the random poisonings of Tylenol capsules, the devastating Exxon Valdez oil spill, the Columbine High School shootings and the crash of a ValuJet flight into the Florida swamps.

Unlike natural disasters, however, human-caused disasters are not inevitable. They do not need to happen. As a result, the general public is extremely critical of organizations who are held responsible for the crises.

Of course, it's impossible to eliminate crises completely. But with the right crisis management (CM) tools — and attitudes — in place, a company can ensure that it can either anticipate crises or effectively manage them once they occur. This summary presents the following fundamentals about crisis management:

- ✓ **The Five Components of a Crisis-Management Framework.** Mitroff and Anagnos present a crisis-management framework that includes five components: types or risk categories of crises; mechanisms; systems; stakeholders; and scenarios.
- ✓ **How Telling the Truth Is Vital to Crisis Management.** The question is not whether the truth will be revealed, but rather when that truth will become public and under what circumstances. Crises only become worse when a cover-up is attempted.
- ✓ **Assume Responsibility or Pay the Price.** If you don't assume responsibility immediately, a chain reaction of crises is guaranteed.
- ✓ **Crisis Management Is an Exercise in Creative Thinking.** Don't go for the obvious response.

Your how-to manual on crisis management begins on the next page.

Published by Soundview Executive Book Summaries, 10 LaCrue Avenue, Concordville, Pennsylvania 19331 USA

MANAGING CRISES BEFORE THEY HAPPEN

by Ian I. Mitroff with Gus Anagnos

— THE *COMPLETE* SUMMARY

The Five Components of a Crisis Management Framework

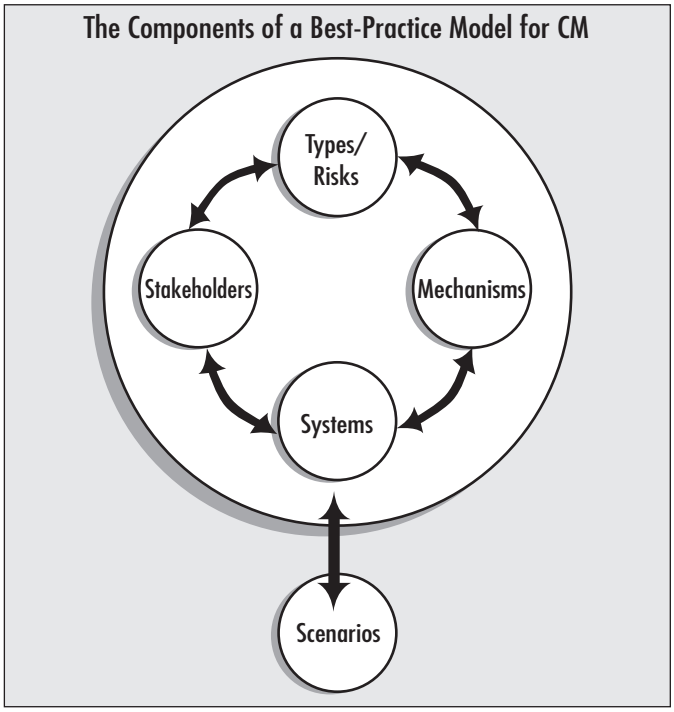
Completely preventing human-caused crises is impossible. However, with the appropriate planning and preparation, any company can limit both the duration and the damage caused by major crises. Effective crisis management also ensures that a crisis or a series of crises does not derail your major business objectives.

Authors Ian Mitroff and Gus Anagnos have developed a best-practice model that identifies the five factors companies must manage before, during and after a major crisis. These five factors are: 1) the types and risk categories of crises, 2) mechanisms, 3) systems, 4) stakeholders and 5) scenarios.

In the first section of this summary, we will look at each of these components in depth.

Types and Risk Categories of Crises

Major crises can be divided into a number of general categories. These categories include:



- **Economic crises**, such as labor strikes, labor shortage, market crash, a major decline in stock price and fluctuations or a decline in major earnings.
- **Informational crises**, such as a loss of proprietary and confidential information, tampering with computer records or a loss of key computer information with regard to customers and suppliers.
- **Physical crises**, such as a loss of key equipment,

(continued on page 3)

What Is a Major Crisis?

It's not possible to give a precise and general definition of a crisis, just as it's not possible to predict with exact certainty when a crisis will occur, how it will occur and why.

We can, however, propose a guiding definition of a major crisis. First, a major crisis affects, or has the potential to affect the whole of an organization. If it is an event that will affect only a small, isolated part of the organization, it may not be a major crisis.

A major crisis will also exact a major toll on human lives, property, financial earnings and the reputation and/or general health and well-being of the organization. Often these effects occur simultaneously. As a result, a major crisis cannot be completely contained within the organization's boundaries.

And some major crises, such as the one suffered by Barron's Bank several years ago, will actually destroy the organization.

The authors: Ian I. Mitroff is Harold Quinton Distinguished Professor of Business Policy at the Marshall School of Business, University of Southern California. He is also president of the consulting firm Comprehensive Crisis Management and was founder and director of the USC Center for Crisis Management. Gus Anagnos is Vice President of Comprehensive Crisis Management.

To subscribe: Send your name and address to the address listed below or call us at **1-800-521-1227.** (Outside the U.S. and Canada, 1-610-558-9495.)
To subscribe to the audio edition: Soundview now offers summaries in audio format. Call or write for details.
To buy multiple copies of this summary: Soundview offers discounts for quantity purchases of its summaries. Call or write for details.
Published by Soundview Executive Book Summaries (ISSN 0747-2196), 10 LaCrue Avenue, Concordville, PA 19331 USA, a division of Concentrated Knowledge Corporation. Publisher, George Y. Clement. Publications Director, Maureen L. Solon. Editor-in-Chief, Christopher G. Murray. Published monthly. Subscription, $89.50 per year in the United States and Canada; and, by airmail, $95 in Mexico, $139 to all other countries. Periodicals postage paid at Concordville, PA and additional offices.
POSTMASTER: Send address changes to **Soundview, 10 LaCrue Avenue, Concordville, PA 19331.**

Types and Risk Categories of Crises

(continued from page 2)

plants and material suppliers, breakdowns of key equipment and plants, loss of key facilities and major plant disruptions.

- **Human resource crises**, such as a loss of key executives, loss of key personnel, rise in absenteeism, a rise in vandalism and accidents and workplace violence.
- **Reputation crises**, such as slander, gossip, rumors, damage to corporate reputation and tampering with corporate logos.
- **Crises resulting from psychopathic acts**, such as product tampering, kidnapping, hostage taking, terrorism and workplace violence.
- **Natural disasters**, such as earthquakes, fires, floods, explosions, typhoons and hurricanes.

As we've already noted, natural disasters do not necessarily have the same effect on an organization, since the general public will rarely see a company struck by a natural disaster as a villain. Of course, if clear mistakes were made — for example, building flimsy factories in earthquake-prone regions — the company's reputation will suffer.

Prepare for One Crisis in Each Category

Within the general categories or types of major crises, the crises share many similarities. Between the categories, there are sharp differences. The best crisis management approach is to try to prepare for at least one crisis in each of the categories.

Most companies, however, do much less. They will consider, at most, one or two categories.

For example, most companies prepare for natural disasters. Organizations that do broaden their preparations for crises other than natural disasters often do it only for "core or normal" disasters that are specific to their particular industry. The chemical industry, for example, prepares for explosions and fires, since these crises are part of the industry's day-to-day operating experience. The same holds true for fast-food companies that prepare for food contamination and poisoning.

While companies have a legitimate reason to be concerned about crises that they know will occur in their particular industry, they must not assume that the crisis they anticipate will be the crisis they will face. The fast-food industry can be hit with a crisis that has nothing to do with food contamination.

In other words, every organization can be hit with a crisis of any of the types listed above. Take product tampering, which was listed under the "psychopathic acts" category. One naturally thinks of the food or the pharmaceutical industries as being particularly vulnerable. But what about publishing?

The Systemic Nature of Crisis Management

A complex system involves a number of intertwined parts working together. The separate parts of the system cannot exist nor function in isolation from one another. For instance, you can't remove the heart or lungs from a human body and have the human body survive. Also, because systems are so tightly interconnected, one event in one part of the system can have system-wide effects.

These characteristics of complex systems are reflected in modern society. We are much more interconnected than before. The impact of one event in our society will have much wider implications than in the past.

For example, 60 years ago, the impact of human-caused crises, such as a mine disaster or an explosion, would have been limited to one particular community or region. Today, crises can impact vast areas of the globe in little time. A rogue trader in the Far East, as was recently shown, can bring down one of the oldest blue-chip banks in the world. Or a nuclear disaster such as Chernobyl can threaten the health of people on two continents.

As a result, crisis management must always include the big picture. For example, ask yourself: "How can I temper how a crisis in one area of the company will impact the entire company?" "How can I prevent one crisis from causing another crisis or a chain of crises?"

The systemic nature of crisis management also means that it must be integrated with other important organizational programs in your company, such as quality assurance, strategic planning, environmentalism or issues management. Crisis management should never be viewed as another separate, stand-alone program.

This is exactly what happened in France to the publishers of the Larousse encyclopedias. The French being avid collectors and eaters of wild mushrooms, Larousse has a page filled with illustrations of mushrooms that are edible and, on the facing page, illustrations of unsafe mushrooms. One year, the labels on the two pages were reversed, causing the unsafe mushrooms to be labeled safe, and vice-versa. This was a case of a product-tampering crisis in an industry probably unprepared for such a crisis.

In sum, as we said earlier, every organization must prepare for at least one crisis in each of the various categories or types.

(continued on page 4)

Types and Risk Categories of Crises

(continued from page 3)

Prepare for Simultaneous Crises

Fortunately, you don't have to prepare for every specific type of crisis within each of the categories. As we noted earlier, each of the specific types within a particular category or type share strong similarities. Of course, the broader range of crises for which you are prepared, the stronger your crisis management capabilities. But in the beginning, it is sufficient to prepare for one particular crisis in each category.

One final and important note: In today's world, any crisis is capable of setting off any other crisis. As a result, companies should prepare not only for each individual crisis they've selected as part of the crisis portfolio, but also for the simultaneous occurrence of multiple crises. In other words, crisis management is strongly systemic. Like total quality management or environmentalism, if it is not done systemically, then it is not being done well. ■

Risk Analysis vs. Crisis Management

Author Ian Mitroff strongly counsels against traditional risk analysis for companies. The reason: Risk analysis mainly selects crises with which the company or the company's industry is familiar. One of the fundamental steps for traditional risk analysis is to construct models of the probability of occurrence of past crises. These models will give a higher ranking to certain types of crises based on how likely they are to occur. Conversely, the models give low rankings to crises that are least likely to occur.

However, it is precisely those crises that have never occurred before that must be anticipated. Yet, using traditional risk analyses, companies will not prepare for a crisis until it happens — at which point, of course, the unprepared company can be significantly damaged.

Mechanisms to Prepare for and Respond to Crises

We now move onto the second of the five elements of our crisis management model: mechanisms.

The best form of crisis management is preparation before the crisis occurs. For this, the company must put in place a small number of mechanisms that will help your company anticipate, sense, react to, contain, learn from and redesign effective organizational procedures for handling major crises.

The first of the mechanisms concerns signal detection.

Signal Detection Mechanisms

All crises send out early warning signals. In many cases, of course, these signals may be weak and camouflaged by noise. But if your company has the mechanisms in place to enable signals to be picked up, amplified and acted upon, then it stands a greater chance of preventing crises before they happen.

For example, make sure that a process exists for front-line employees to be able to communicate with management about their concerns. After the tragic explosion of the space shuttle Challenger cost seven lives, it was discovered that a string of memos expressing concern about the design of the shuttle were ignored by management.

The Signal Detection Chain

Dr. Judy Clair of Boston College did extensive research on signal detection in a large insurance company. This company handled billions of dollars in government Medicaid payments. The threat of fraud was extremely high.

Based on her research, Dr. Clair developed the important links in the "signal detection chain."

The first link: the signal detector.

Hearing the Signal

If a company wants to detect signals, it must have signal detectors. Although this may sound obvious, most companies do not have signal detectors in place. In other words, signals of an impending crisis may be clearly visible, but no one is paying attention.

The intensity threshold must also play a role. A signal detector must be able to read a signal and determine whether it has reached a level of intensity that indicates danger or potential danger for the company.

Because different types of crises send out very different types of signals, each company must ask itself: "What would count as a signal of the impending or near occurrence of a particular type of crisis?"

One example might be a pattern of slow, but noticeable increases in the accident rate at a particular oil refinery; this pattern may signal an impending serious accident, such as an oil spill, fire or explosion.

Of course, if there is no one or no mechanism recording the accidents, then the pattern remains invisible. The signal goes undetected.

There must also be someone at the refinery or at headquarters to read the accident reports and note the pattern. If signals go off but there is no one to recognize, record and attend to them, the signals are not heard.

(continued on page 5)

Mechanisms to Prepare for and Respond to Crises

(continued from page 4)

Signal Transmission

Once the signal is heard, the next step is to transmit the signal to the right people (and in the right form). If someone picks up a signal in your company but doesn't know to whom to send it, or sends it to people who don't know what to do with it, then, once again, the signal will fail.

In sum, it is important, when putting in place signal mechanisms, to:

- **have signal detectors in place that can pick up the signals;**
- **have intensity thresholds established so that people know when a signal indicates a dangerous situation for the company;**
- **clearly communicate what people should do with a signal when it is detected.**

One final note on signal mechanisms: It is not enough to pick up individual signals from different locations. It is possible that only when two signals are combined does the danger to the company become evident. Companies must be prepared to have a gathering point for signals, in other words, a central location where the signals can be pieced together into a larger whole.

Other Mechanisms

Without proper signal detection mechanisms in place, an organization not only makes a major crisis more likely, but also reduces its chances of bringing it under control when it does occur.

Even with the best signal mechanisms in place, however, crises will occur. Thus, your company will also need damage containment mechanisms to keep the unwanted effects of the crisis from spreading. Of course, a damage containment mechanism that is appropriate for one type of crisis will not necessarily be appropriate in containing others. A systemic and systematic CM program will feature a number of damage containment mechanisms.

Finally, your company must also have postmortem mechanisms in place that will allow it to learn from the crisis and redesign the systems and mechanism to improve crisis management in the future. Few organizations conduct postmortems of crises and near-misses — and those that do either do not perform them correctly or don't implement their findings.

When doing a postmortem, the goal is not to assign blame. It is to examine the key lessons that need to be learned. The exception, of course, is in crises that involve criminal malfeasance or negligence. ■

Four Types of Signals

Signals can be differentiated along two dimensions. The first dimension relates to the source of the signal. In this dimension, signals can either originate from inside or outside the organization.

The second relates to the kind of signal. Signals can be either technical (recorded by remote sensing devices), or noticed by people.

If you put these two dimensions together, you have four types of signals that apply to every company:

1. Internal technical signals, such as monitoring devices for hazardous operations.

2. Internal people signals, for example, people working in a plant.

3. External technical signals, such as monitoring of plant emissions carried out by environmental activist groups.

4. External people signals, including members of surrounding communities who may literally "smell" that something is wrong.

Organizational Systems

The third component of the crisis management framework involves organizational systems.

A company and its various systems can be illustrated as the layers of an onion (see box next page). The outermost layer is technology. Then come organizational structure, human factors, organizational culture and finally, at the core of the organization, top management psychology. These are the systems that govern most complex organizations.

A company's systems are intertwined, interacting with one another in many ways. Complex technologies, for example, are run by humans and thus are susceptible to human errors. Technologies are also embedded in complex organizational structures. These complex structures can also lead to errors as messages and communications must travel across different and multiple layers.

Organizational Culture

Organizational culture is a critical component of the systems involved in crisis management. For example, an organizational culture that establishes reward systems that reward certain kinds of behavior can hinder communication to the right people — and, thus, lead to wrong decisions.

One example of the impact of organizational culture on crisis management involves a power utility that

(continued on page 6)

Organizational Systems

(continued from page 5)

served extreme northern settlements. If the power failed, the inhabitants of these communities would literally freeze to death within 36 hours.

The most likely employees of this power utility to find flaws in the electrical generators that served these communities were maintenance workers. Maintenance workers were the signal detectors; they filled out logs at the end of each shift on the state of the generators. However, the culture of this power utility placed maintenance workers at the lowest rung of the company. Therefore, their logs were ignored and their warnings were not taking seriously.

The most prestigious jobs in the company belonged to the linemen, those who climbed the poles to repair the lines. The linemen were macho risk-takers — in fact, they made a point never to wear safety equipment.

Obviously, the macho culture of this organization made it susceptible to a variety of crises.

A Defensive Corporate Culture

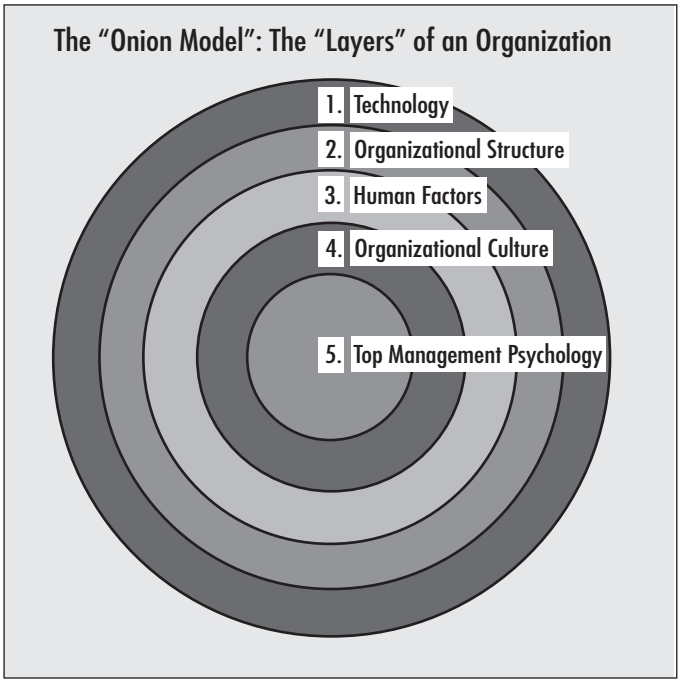
The impact of a company's organizational culture on crisis management is also apparent when we look at one of the key components of a culture: defense mechanisms. As with humans, organizations have defense mechanisms that rear up to deny vulnerabilities to major crises. These defense mechanisms can take many forms, including denial ("Crises only happen to others,") disavowal ("Crises happen, but their impact on our organization is small,") grandiosity ("We are so big and powerful that we will be protected from crises") or compartmentalization ("Crises cannot affect the whole of our organization since the parts are independent of one another.") ■

Don't Forget Your Stakeholders

The fourth element of your organization that must be involved in crisis management is the company's stakeholders.

Stakeholders include all of the internal and external parties who cooperate, share crisis plans and participate in the training and development of your company's crisis management capabilities. Stakeholders can range from your employees to such external agencies as police departments, fire departments and even the Red Cross. Another important external stakeholder is the media, which will not hesitate to judge harshly an inadequate response to a crisis.

Crisis management must include developing the right relationships with stakeholders in advance to ensure the smooth functioning of the organization in the heat of a major crisis.



Make-a-Wish Foundation and its Stakeholders

The importance of understanding stakeholders in crisis management is illustrated by a story involving the Make-a-Wish Foundation. This well-respected organization grants wishes to terminally ill children. One child, a teenager suffering from a brain tumor, wished to hunt a Zodiac bear in Alaska. When the foundation enabled the teenager to achieve his wish, it suddenly found itself under fire from numerous animal-rights organizations and portions of the general public. The foundation's mistake involved several assumptions about the organization's stakeholders. The first assumption was that the primary stakeholder was the teenager, and that other stakeholders (including the general public which supports the group through donations) would not object to the wishes of the teenager, despite any ethical or moral qualms they might have. The Foundation believed those stakeholders would share the foundation's view of the situation: Make-A-Wish had to find a way to grant the wish of a dying child as effectively as possible no matter how offensive it may be to others.

Several crisis management lessons can be drawn from this example. First, never assume the outside world sees a situation exactly as you do. Second, it's a good idea to list as many assumptions as possible about as many stakeholders as you can think of. Be careful not to overlook any stakeholders, or to accept any unwarranted assumptions about stakeholders.

This story also highlights another important point about crisis management situations: Don't solve the wrong problem precisely. The foundation focused on finding a way to fulfill the teenager's wish. Solving that problem led to the crisis. ■

You Are Now Ready to Develop Crisis Management Scenarios

Taking into account all of the four elements of the crisis management framework we've discussed above — types of crises, mechanisms, systems and stakeholders — your company can develop the fifth and final component of the framework: scenarios.

What will happen if a certain crisis occurs? How will your organization and its employees and customers react? What steps will have to be taken? These are the kinds of questions that must be answered in a scenario.

The best approach is to create a "best-case, worst-case" scenario. In the best-case scenario, of course, everything goes as planned in response to the crisis — a crisis that was anticipated. A worst-case crisis scenario, on the other hand, involves a type of crisis that the organization has neither considered — and for which it is not prepared. Also, the crisis occurs at the worst possible time — over a holiday weekend, for example. And the most taken-for-granted, well-designed and well-performing systems break down.

To summarize the framework presented by Ian Mitroff and Gus Anagnos, effective crisis management means:

- understanding and preparing for the different types of crises;
- implementing the important mechanisms that will help you prepare for those crises;
- understanding the impact of your company's systems — from organizational structure and culture to human factors and the psychology of your top management — on crisis management;
- developing the right relationships with stakeholders in advance of a crisis;
- establishing best-case, worst-case scenarios.

These five components should be used as a framework for an audit of your company's crisis management program. A crisis audit will reveal any weaknesses in one or more of these areas that might hinder your crisis management capabilities. ■

How Telling the Truth Is Vital to Crisis Management

The general framework presented here is a key tool in crisis management. But by itself, no framework, while necessary, is sufficient. In addition, crisis management must confront the question of both individual and organizational character. Specifically, crisis management must address two questions:

1. Do we (the individual, the organization) always tell the truth?

2. Do we (the individual, the organization) always assume responsibility?

This article deals with the first issue: telling the truth.

Should the Public Know?

The question is not whether you or your company should lie or tell the truth. The question is: When a crisis occurs, how much of the truth must be made public? Should a company try to fix the crisis in-house, sheltered from prying eyes? For example, if a CEO is caught in a compromising position, should that CEO be fired without any explanation? Or should every detail be made public?

There are no easy answers. But here's an important consideration: In today's society, there are no secrets anymore. None. Technology in general, and television in particular, has invaded every "back-stage" that might have once existed in the lives of people and institutions. For example, overzealous police officers might have once been able to step over the limit in their behavior without being caught. Today, police brutality is likely to be captured on videotape by passersby or hovering television cameras. Human rights organizations are even distributing free video cameras to citizens in countries with poor human rights reputations so that they can film incriminating acts by their governments.

By taking the initiative, you (or your organization) controls who reveals the truth, in what circumstances and when.

The question, therefore, is not whether the truth about an organization or individual will be revealed, but rather when that truth will become public and under what circumstances.

In light of this situation, the best approach is to take the initiative to tell the truth about a crisis. By taking the initiative, you (or your organization) controls who reveals the truth, in what circumstances and when. Ian Mitroff describes the advice he offers his clients on telling the truth:

"No matter what the crisis situation, I always advise my clients to tell as much of the truth about themselves as they are able and willing to tell. I next ask them to take the additional step and tell a bit more, and a bit more, etc. Only after both of us are satisfied that they have indeed told 'enough' of the truth to ensure that the crisis will not be perpetuated any further can they finally stop. In short, how much 'truth' do I tell my clients to reveal about themselves? More than they can stand to bear, but, unfortunately, not what the world wants to hear and to gloat over!" ■

Assume Responsibility Or Pay the Price

The next issue concerning character and crisis management is whether or not to assume responsibility. In this case, the answer is clear and unequivocable: Yes. You or your organization should always assume full responsibility.

In a crisis situation, a company will fall into the role of villain — someone who knowingly causes harm or allows harm to happen.

Villains, however, fall into different categories. "Repentant" villains accept full responsibility for the crisis, promise to correct the situation and to prevent the situation from ever reoccurring, then take action to back up their promises. One example is Lee Iacocca's response to the substantiated charges that Chrysler was falsely resetting odometers on its cars: "It happened; it shouldn't have happened; it won't happen again."

Unlike repentant villains, "damn" villains are those who knowingly cause harm and then deny that they did it. In other words, they refuse to assume responsibility for their actions. Those who continually engage in stonewalling and denial are what Mitroff calls "damningly, damnable villains." They not only created a crisis in the first place, but their stonewalling sets off a chain reaction that causes additional crises. Or to put it more bluntly, if you don't assume responsibility from the very beginning, a chain reaction is virtually guaranteed. The classic case, of course, is Watergate, in which one isolated incident snowballed until it brought down a sitting U.S. president. ■

Crisis Management: An Exercise in Creative Thinking

Crisis management requires individuals and companies to think about the unthinkable. It is, in other words, an exercise in creative thinking. Creative thinking is especially important in preventing a crisis from escalating into a worse situation.

In this article, we present two case studies showing the power of creative thinking in responding to crises.

Why Benetton Erased Its Colors

In 1999, an international incident arose between the Turkish and Italian governments over the fate of Kurdish rebel Abdullah Ocalan, who had fled to Italy. When the Italian government refused to extradite Ocalan to Turkey, Italian businesses and products in Turkey, including Benetton, Ferrari and Perelli, were the targets of widespread and violent protests. Many Italian businesses took out newspaper ads pointing to the difference between an Italian parent company and the Turks who operated them. Benetton-Turkey took a different tack. To show its solidarity with the Turkish people, Benetton-Turkey's "corporate response team" — consisting of the president, head of public affairs and head of corporate finance — developed a crisis plan that was as creative as it was effective. The plan involved going to the heart of Benetton's corporate identity — the logo, "The United Colors of Benetton" — and making a statement by removing those famous colors. In addition to removing the colors from its logo, black wreaths were place on the storefronts of all Benetton stores throughout Turkey until the situation was resolved. Also, all of the mannequins in the store windows were dressed in black indicating that the company was in a state of mourning.

Benetton-Turkey's response was exemplary in many ways. Not only was it swift and dramatic, but it recognized than an emotional response, not the logical and rational response of the other businesses, was key in diffusing the crisis. Responding emotionally, and doing the unthinkable, allowed Benetton-Turkey from becoming a hated villain.

Talking Down the Greens

Another example of thinking creatively involves the Swiss chemical conglomerate CIBA. Two German Green Party activists climbed a 600-foot smokestack and unfurled a huge banner declaring that CIBA was harmful to the environment. Rather than following the typical heavy-handed response of having the protesters forceably removed (which would only bring more publicity to their cause and create more enemies), Walter von Wartburg, head of Issues Management for CIBA, sent an emissary up the smokestack to ask them to come down and talk about their issues with him. They were told they could leave their banner up. The two Greens eventually came to talk with von Wartburg over tea.

The lesson of the story: Before adopting any solution to a problem, always ask, "Is the proposed solution likely to create even worse problems?" ■

Needed: One Champion

For an organization to successfully instill a crisis management program, it must find an organizational champion to lead the way. This champion should be a leader who has championed other system-wide programs. He or she must be able to see the big picture and make the connections between the various parts of the organization. The champion also needs to understand and be able to explain to top executives how a major crisis will derail the major business objectives of the company.