Center for
Effective
Organizations

COPING WITH EVIL: THE NEW CHALLENGE OF CRISIS MANAGEMENT

CEO PUBLICATION
G 03-14 (442)

IAN I. MITROFF

Center for Strategic Public Relations
Annenberg School for Communication
University of Southern California

MURAT ALPASLAN

University of Southern California

March 2003

Coping with Evil:
The New Challenge of Crisis Management

by

Ian I. Mitroff
The Harold Quinton Distinguished Professor of Business Policy
The Marshall School of Business
Professor of Journalism and
Director, USC Center for Strategic Public Relations
The Annenberg School for Communication
University of Southern California
Los Angeles, California, 90089

President,
Comprehensive Crisis Management
Manhattan Beach, CA 90266
310-372-3418
ianmitroff@earthlink.net

and

Murat Alpaslan
Doctoral Candidate
Marshall School of Business
University of Southern California
Los Angeles, California, 90089

2002 is the twentieth anniversary of the Tylenol poisonings, the single crisis that more than any other event is associated with the beginning of the modern field of Crisis Management (CM). In appraising the lessons that have been -- and even more importantly, "should have been"-- learned during the twenty years since the Tylenol poisonings, the following questions are critical. Indeed, after 9/11 they have become urgent: "Have there been significant changes in the ways that companies adopt and implement CM?"; "What do the best companies do with regard to CM?"; "Are there 'best practices' that can be clearly identified?"

Recent Crises

From a CM perspective, the last twelve to eighteen months have been extraordinary. As a society, we went directly from the Ford/Firestone tire debacle (May to September, 2000) into 9/11/2001. This was followed in close succession by unsavory revelations that Catholic priests had committed serious acts of child abuse, and furthermore, that these acts were repeatedly covered up by the Church; massive fraud by the top executives of Enron and Andersen; serious allegations that both the CIA and the FBI failed to do their basic jobs in compiling terrorist information such that if it had been collected and gotten to the right persons at the right time, then conceivably 9/11 might have been prevented altogether; in addition, serious breakdowns in communications occurred within the FBI and the CIA so that an accurate portrait of terrorist intentions could not

be formed within their respective agencies, let alone an integrated portrait that could have been formed by sharing information between them.

It is tempting to dismiss the crises that happened to the FBI and the CIA because on their surface they do not apply to businesses. However, as we shall shortly see, the best businesses take every crisis seriously no matter to whom it happens. In short, every crisis is an opportunity to learn from the experiences of others. Because of the tremendous impacts that 9/11 had on the businesses that were quartered in the Twin Towers, and the general economy, all crises, whether they happen in the so-called public or private sectors, increasingly impact one another. In a word, all crises are interdependent.

When it surfaced that the top executives of Adelphia, World Com, and Tyco had engaged in criminal and fraudulent behaviors, then the crises in the previous paragraphs were followed in quick succession by a plummeting stock market. Furthermore, corporate heroes and major cultural icons such as Martha Stewart and Jack Welch had their reputations tarnished seriously as the result of "corporate improprieties."

While none of the preceding crises necessarily "caused" one another—with the possible exception of the relationships between (a) the loss of confidence in the auditing and stock analyst professions, (b) the criminal behavior of a few highly visible CEOs, and (c) serious drops in the stock market—they led nonetheless to major drops in consumer confidence and a general lowering of trust in all of our major institutions as evidenced by the wealth

of stories in the major news and business publications. In this way, they became a "collective crisis" because they were a severe blow to the nation's psyche.

The State of CM in Corporate America

For over twenty years, Mitroff and his colleagues have conducted periodic survey of the Fortune 1000 companies with regard to their CM behavior and performance. They have also conducted over 30 CM audits of major organizations. The organizations have spanned every type of industry and sector of the economy. They have also included private, public, and governmental organizations as well.

One of our latest surveys just happened to have been sent out prior to 9/11. After 9/11, we immediately sent out a follow up survey. In addition, we also sent out a survey on the one year anniversary of 9/11 to see what organizations had learned and internalized.

The surveys of the Fortune 1000 companies before 9/11, immediately after, and one year later provide extremely compelling evidence that effective CM along with an appropriate ethical base are "good for business." Prior to 9/11, we found that the vast majority of businesses were largely unprepared either for terrorism or large-scale accidents, for example, a major crisis that would destroy an entire high-rise building or large manufacturing plant that was spread out over several city blocks. After 9/11, the general preparedness for all crises increased dramatically, especially with regard to preparation for terrorism and large-scale systems accidents. One year later, we have found the same increased levels of

crisis preparedness have been maintained. However, the underlying reasons for engaging in CM vary dramatically.

Over the years, we have found that organizations can be classified into two broad types with regard to their CM behavior and performance: Proactive versus Reactive. The differences between these two types of organizations are as follows: Proactive organizations anticipate and prepare for a larger number and a wider variety of crises (see Table 1) than the crises they have already experienced! In contrast, Reactive organizations prepare for a smaller number of crises than the ones they have experienced! Thus, an easy way to differentiate between these two is to subtract the number of crises an organization has already experienced from those it is prepared for. This number is positive for Proactive organizations, negative for Reactive.

Before 9/11, 61% of the organizations responding to our survey were Reactive; 39%, Proactive. (A total of 1,000 questionnaires were sent to the heads of HR, Legal, and Security of the Fortune 1000; another 1,000 immediately after, and 1,000 one year later. The respective response rates were 5%, 6%, and 8%. These rates of response are in line with other types of questionnaires which probe for extremely sensitive and confidential information; however, what is most important is that the response rates were representative of the various types of industries in the population.) Immediately after 9/11, 46% of the sample could be classified as Reactive; 54% as Proactive. One year after 9/11, 39% could be classified as Reactive; 60% as Proactive. Thus, we see

Table 1:
MAJOR TYPES OF CRISES

Economic	Informational	Physical (Loss of key plants and facilities and products)	Human Resource
Labor strikes Labor unrest Labor shortage Major decline in stock price and fluctuations Market crash Decline in major earnings Hostile takeovers	Loss of proprietary and confidential information False information Tampering with computer records Loss of key computer information with regard to customers, suppliers, etc. Y2K	Loss of key equipment, plants, and material supplies Breakdowns of key equipment, plants, etc. Loss of key facilities Major plant disruptions Explosions Faulty or poor product design Product failures Poor quality control	Loss of key executives Loss of key personnel Rise in absenteeism Rise in vandalism and accidents Workplace violence Lack of succession plans Corruption
Reputational	**Psychopathic Acts**	**Natural Disasters**	
Slander Gossip Sick jokes Rumors Damage to corporate reputation Tampering with corporate logos False rumors	Product tampering Kidnapping Hostage taking Terrorism Workplace violence Criminal/ terrorist/ psychopathic acts	Earthquakes Fires Floods Typhoons Hurricanes Mudslides	

clear and dramatic shifts in the general CM behavior of the Fortune 1000.

These differences have profound effects on the CM behavior of organizations. It also has profound effects on their financial performance. For instance, we found that overall, Reactive organizations experienced an average of 33 crises (see Table 1) during the time period immediately preceding 9/11 until one year later. In contrast, Proactive organizations experienced an average of 21 crises. In other words, Reactive organizations experienced at least 50% more crises than Proactive. This difference not only impacts their bottom line, but also their standing in the Fortune 1000 Most Admired list.

The average Return on Assets (R.O.A.) of Reactive organizations was 3.0%. In comparison, the average R.O.A. of Proactive organizations was 6.0%. While not all of this can be attributed to effective CM, from previous studies, there is no doubt whatsoever that part of the improved R.O.A. of proactive organizations results from the lesser costs that they incur due to major crises. For instance, the Ford-Firestone tire crisis is reputed to have cost both Ford and Firestone at least $500 million dollars.

On average, Reactive organizations have a standing on the Fortune 1000 list of 5.6; Proactive, 6.2, where 1 represents the worst score and 8 the highest. All of these factors combine to make the average age of these two types of organizations dramatically different as well. The average age of Reactive organizations is 67; that of Proactive, 83.

Immediately after 9/11, Reactive organizations dramatically increased their preparations for all types of crises because, “It was the right thing to do.”

One year later, Reactive organizations are maintaining their levels of crisis preparedness, but, “Only if it is cost effective.” Proactive organizations did not dramatically increase their crisis preparations after 9/11 because they were already operating at a high level of CM effectiveness. Reactive organizations were thus largely responsible for the sharp overall increase in CM preparedness.

The differences between these two types of organizations extend far beneath their surface or immediately visible behavior. Proactive organizations operate by the ethical principle, “Do no harm even to a single person.” Indeed, this principle permeates their entire culture and their business practices. As a result, it not only leads Proactive organizations to take safety considerations extremely seriously, but other programs such as Total Quality Management, Environmentalism, etc.

In contrast, Reactive organizations operate by the ethical principle, “Do the greatest good for the greatest numbers of people.” In other words, Proactive organizations are guided largely by an ethical orientation that says, “Do the right things irrespective of their costs.” In contrast, Reactive organizations are guided by, “Do what is right, but if and only if it is cost effective.”

While Reactive organizations are guided almost entirely by cost considerations, they are substantially less profitable than Proactive organizations as indicated by their R.O.A.’s! Effective CM and ethics not only go hand in hand, but they pay off handsomely. In a word, they are good for business. These findings should make business school faculties and executives ponder seriously, and give serious reconsideration, to the value of teaching business ethics. In

other words, ethics is not separable from CM. Indeed, it is an integral component of effective CM.

Crises: Normal, Abnormal, and Natural

In 1984, the distinguished Yale sociologist Charles Perrow published a highly influential book with the enticing title, Normal Accidents: Living with High Risk Technologies (Basic Books, New York). Through detailed, critical studies of the airline, chemical, nuclear, and shipping industries, Perrow concluded that the potential for major crises and catastrophes was literally built into their basic operating structures. Major crises and catastrophes were virtually guaranteed to occur because the management systems that were in place were not up to handling the complexities of the technologies involved. It was in this special sense that catastrophic accidents were "normal." In other words, major accidents and crises were not isolated, random aberrations. Instead, they were a "normal part" of the everyday operations.

While Perrow certainly envisioned the possibility of terrorism, for instance, directed against nuclear power plants, it was not yet the major force that it has become, especially after September 11, 2001. For this reason, Perrow did not envision what we would call Abnormal Accidents, certainly not on the scale that we have experienced recently.

If Normal Accidents are the result of unintended systems complexity, then Abnormal Accidents are the result of intended evil, or Evil Intentions. In slightly different words, if Normal Accidents are the result of the unintentional

breakdown of complex systems due to their faulty design and inadequate safety procedures, then Abnormal Accidents are due to the breakup of complex systems due to deliberate evil actions.

In addition, there are of course Natural Accidents, i.e., crises that are due to natural disasters. Furthermore, each of the various types, Normal, Abnormal, and Natural are not necessarily distinct; they can overlap. Nothing prevents them from occurring simultaneously and from each setting off or affecting the others.

Types of Accidents and Crises

Table 1 shows a broad and diverse array of different Types of crises. It shows that different Types fall into a relatively limited and small number of groups or "crisis families. Proactive or Crisis Prepared companies form a CM Portfolio that includes at least one crisis from each of the known crisis families in Table 1. That is, Crisis Prepared companies prepare for the occurrence of at least one crisis in each family. In this way, they use a "rational strategy" to acknowledge and to spread their risks. They prepare and think broadly about the full range of crises that can happen to any organization. In addition, they do something that is equally important. They "connect the dots" because it has been found repeatedly that no single crisis ever occurs in isolation.

Any crisis in any family can either be the cause or the effect of any other crisis in any other family. Every crisis is capable of setting off a chain reaction of other crises. Consider, for instance, 9/11. To put it mildly, 9/11 was a

terrorist act of unparalleled magnitude. However, it also set off all kinds of additional crises, for example, those in the "economic family." 9/11 directly affected the airline industry in general and the tourism business in particular in California.

Since in today's world, it is no longer sufficient to plan for individual crises in isolation, Crisis Prepared companies thus construct multiple scenarios and carry out simulations that include the simultaneous occurrence of widely varying crises. An important example of this is a major OPEC company. (Because of the extreme sensitivity of CM, the identities of most of the companies with whom Mitroff and his colleagues have worked cannot be revealed.)

A top executive of a major OPEC company showed how each of the individual crises that his industry faced could easily become part of an overall pattern and chain reaction that could happen to his particular organization. For example: (1) falling prices for oil on world markets, a major crisis in and of itself, would lead the company to (2) lay off workers. In turn, this would (3) anger its unions. This could result in (4) increased acts of workplace violence and sabotage which would (5) damage the refineries, thus (6) further lowering their production capacity. This would (7) necessitate laying off of additional employees. As a result, it was very easy for the company to fall into a dangerous and vicious loop of multiple crises.

In addition to "connecting the dots," this particular executive also indicated what would be strong early warning signals such that if a particular

crisis in the chain occurred, then another was about to occur. This is especially important since virtually all crises send out far in advance of their actual occurrence a trail of early warning signals. Thus, as part of their being proactive, Crisis Prepared companies attempt to pick up, to amplify, and to get the signals to the right persons in the right places so that the right preventative actions can be taken.

In this way, the executive of this particular OPEC company anticipated various crises and attempted to respond to all of them proactively. For instance, steady or sharp increases in absenteeism, graffiti on bathroom walls, and sick jokes uttered with regard to the organization were all potential "indicators" or early warning signals of the probability that workplace violence or sabotage was high, i.e., about to occur. These same indicators were also early warning signals of the rising anger of labor unions.

Table 2 also shows that the different Types of crises can be either Normal or Abnormal depending upon whether they are the result of unintended versus intended actions. For instance, false information in computer records may be due to the malfunction or breakdown of equipment and/or faulty procedures. In this sense, they can be unintentional. On the other hand, false information produced by tampering is an example of an Abnormal Accident. It is the result of the intentional break up of systems.

Table 2:
TYPES OF ACCIDENTS AND CRISES

Types of Accidents	Types of Crises
Normal	Economic Informational Physical/Product HR Reputational
Abnormal	Economic Informational Physical/Product HR Reputational Criminal/Psychopathic/Terrorist
Natural	Earthquakes Fires Floods Typhoons Hurricanes Mudslides

Table 2 shows that Economic, Informational, Physical/Product, HR, and Reputational crises can be due either to Normal or Abnormal Accidents, or actions. On the other hand, Criminal/ Psychopathic/ Terrorist Types of crises fall squarely within the category of Abnormal Accidents because they are the result of intended actions by unsavory actors. In addition, there are of course Natural accidents, i.e., acts of nature.

Since Abnormal Accidents are the result of evil intentions, they are generally so distasteful and beyond the bounds of ordinary moral comprehension that they are regarded as "utterly unthinkable" for the vast majority of people. It is precisely for this reason that they demand special skills for their treatment.

A further complication is the fact that extreme overlaps between Normal, Abnormal, and Natural Accidents are possible. Consider, for instance, earthquakes. While earthquakes can neither be predicted nor prevented, how we plan for and respond to them is under human control. Furthermore, the worst effect of earthquakes occurs when they are involved with Abnormal Accidents. For example, consider the earthquakes that occurred in Turkey in recent years and which led to the collapse of high-rise apartments. The earthquakes were especially devastating because the apartment buildings were the result of shoddy design and construction practices. Thus, although humans were certainly not responsible for the cause of the earthquake, nonetheless, humans played a central role in the crisis due to the actions of unscrupulous building contractors.

A Working Definition of "Crises"

Up to this point, we have deliberately resisted defining the term "crisis" for several reasons. For one, there is not universal agreement with regard to its definition. Most important, the definition of what is a "crisis" cannot be used to predict whether a particular crisis will occur or not. Nonetheless, there is some broad agreement regarding the outlines of the definition.

A crisis is "any event which has the potential for causing an organization or an institution literally to go out of business or to cease to exist." A prominent example is Enron and Arthur Andersen. In addition, a major crisis is "any event which exacts major financial costs, causes major deaths and injuries, and has the potential to cause serious damage to the reputation of an organization or individuals."

Further Differences Between Crisis Prepared and Crisis Prone Companies

Crisis Prepared companies do not preoccupy themselves with the definitions of what is and what is not a crisis. Instead, Crisis Prepared companies stress the importance of crisis capabilities over crisis plans. In other words, they focus on developing and refining the actual skills necessary to manage crises before, during, and after major crises. These skills include: (1) conducting regular, periodic audits of the crisis vulnerabilities and the strengths of an organization so that they can assess its potential for crises of all kinds; (2) designing and putting into operation appropriate damage control mechanisms which limit the spread and the resultant damage of major crises; (3) designing,

testing, and implementing early warning signal detection systems for impending crises; (4) setting up alternate work locations and work sites in the event that one's plants and facilities are destroyed or incapacitated; (5) training for communicating effectively with the media and a wide variety of internal and external stakeholders prior to the occurrence of major crises; (6) designing and implementing appropriate reward systems and an appropriate corporate culture which sends a clear signal with regard to the importance of CM.

Crisis Prepared companies stress the importance of crisis capabilities over crisis plans for, more often than not, crisis plans merely sit on shelves and are not rehearsed until they are necessary. By this time, it is too late to implement them correctly. The general thinking of Crisis Prepared companies is that any activity that is important for the day-to-day conduct and operation of an organization, not to mention its very existence, is important enough to be practiced on a regular and periodic basis. Even more, it is important enough to develop working capabilities.

Crisis Prepared organizations also understand that since no crisis ever happens exactly as it has been planned for or simulated, it is not important to include every conceivable type of crisis in one crisis portfolio. In fact, it would be a virtual impossibility to even attempt to do so. What is important is that one should include <u>at least one type</u> from every crisis family whether any member of a particular family has occurred within one's organization, industry, or society. The goal is to have at least thought about the unthinkable as broadly as possible prior to its occurrence. From previous research conducted by the authors and

their colleagues, it has been found that those organizations that are prepared for at least one type of crisis in every family recover at least one third faster and at substantially less cost than those organizations that are not prepared. Thus, once again, an integrated and a systemic approach to CM literally "pays off." (See also the previous section on survey results prior to 9/11, immediately after, and one year later.)

In contrast, Crisis Prone organizations prepare for a narrow and a limited set of crises. If they even prepare at all, it is mainly only for natural disasters, fires, explosions, and already known crises that are part of their day-to-day operations and industry. In short, they prepare for high probability, high consequence disasters and crises. Low probability but high consequence crises such as 9/11 don't make it onto their radar screens because they have not happened in the past.

To further demonstrate the differences between Crisis Prepared and Crisis Prone organizations, consider how they approach a specific crisis such as product tampering. Every organization is subject to product tampering, not just those companies in the food and the pharmaceutical industries. The case of La Rousse, the French manufacturer of encyclopedias is extremely instructive in this regard.

The French are avid eaters of mushrooms. As a result, they take their La Rousse's with them into the forest to determine which mushrooms are safe to eat and which are not. In one part of its encyclopedia, La Rousse literally has two pages side by side. On one page is a picture of all the mushrooms that are

safe to eat. On the very next page are pictures of the mushrooms that are highly dangerous to consume.

For some unknown reason, whether accidental (i.e., Normal) or intentional (i.e., Abnormal), the labels on the two pages were reversed. Thus, the "safe mushrooms" were labeled "unsafe," and vice versa. This is a prime example of product tampering.

Since every organization has important computer databases, and furthermore, since these systems are more vulnerable to break-ins, and hence to altering and tampering with the information contained in them, this means that every organization is now subject to product tampering. In turn, this means that every organization needs to construct scenarios that involve those forms of tampering that are specific and unique to its plants, products, and services. Thus, instead of assuming that one's businesses are immune to tampering, Crisis Prepared organizations flip this basic assumption on its head. Crisis Prepared organizations start with the converse premise, i.e., that tampering is not only possible, but that it has already occurred to them. The only thing that is unknown are different scenarios regarding how tampering could occur.

Creative Demolition

Thinking about crises is difficult precisely because it forces us to challenge explicitly many, if not all, of our basic and deeply held assumptions about ourselves, our companies, industries, and even society. For this reason, thinking about the unthinkable is an extreme exercise in the creative demolition

of our basic assumptions. As a result, it calls for highly unusual exercises in creative thinking.

Because of the demand for confidentiality, we need to emphasize once again that in all of the examples that follow, the organizations have been deliberately disguised. For these same reasons, a few of the examples are composites.

The Internal Assassin Team Exercise

In several organizations with which Mitroff has consulted, he has taken them through a process known as The Internal Assassin Team Exercise. Since the members know more about their own organizations than Mitroff possibly ever could, he has formed them into various teams to come up with the most creative, and yet plausible, schemes and scenarios by which they could do the most damage to their organizations while remaining undetected for the longest possible periods of time.

For instance, Mitroff helped a billion dollar insurance company with over 5,000 employees set up three special assassin teams to attack its businesses. An initial, daylong workshop was held with 24 senior executives at the company's headquarters. Each team was composed of approximately 8 members.

One team was deliberately charged with the goal of coming up with schemes to attack the organization entirely from the inside. That is, how crooked employees working entirely from the inside could tap into the company's computers and siphon off unlimited amounts of money. Another team looked at

how the organization could be attacked primarily from the outside, for instance, by crooked doctors submitting phony bills for payment. A third team took a "mixed" approach. Their strategy was a combination of crooked internal employees acting in collusion with crooked doctors on the outside.

Since significant portions of the organization dealt with Medicaid insurance, literally hundreds of millions of dollars flowed through the organization annually with regard to Medicaid payments. Since the stakes were extremely high, the top executives of the company made the reasonable assumption that if they had not gotten wind of the latest insurance scam, it was not because it was not happening, but rather, it was only because they were unaware of it. As a result, the executives were always on the lookout for the latest scams.

What they had not done was to use their own experience in uncovering scams to look for new ones both systematically and systemically. This is exactly where the Internal Assassin Team Exercise entered. After each of the teams had developed and presented various schemes, all of which were feasible (for instance, the external team concocted a scheme where various doctors were in cahoots with one another and hence formed a "ring"), counter-terrorist teams were then set up to see if they could come up with scenarios to expose and to block the original schemes.

The company soon learned to its chagrin that the most feasible scam for which it was <u>not</u> prepared was as follows: If a potential scam artist was very patient, and somewhat paradoxically, not very greedy, or at least not in the short run, then by very carefully siphoning off small amounts of money over long

periods of time, one could in fact accumulate considerable sums. This led the executives to take serious steps to lower the "threshold of detection" for new scams. They did this by over the coming months investigating new audit procedures that would look for potential problems with lower payouts both to patients and to medical doctors. That is, they set up new "red flag procedures" for lower transactions than they had considered previously. As a further consequence, they also began to investigate new computerized systems and software, which of course themselves could be scammed, to see if they could push the threshold for audits lower and lower.

Detecting scams is like painting the Golden Gate Bridge. It is a process, not an event. It is never finished. It demands continual, on-going vigilance.

Envision Your Business As Being in a Different Industry

Since the operating conditions of different businesses and different industries vary differently, they face different crises on a day-to-day basis. For instance, one does not have to prod the members of the chemical industry to prepare for dangerous explosions and fires since they "come with the everyday territory." They are common, frequently occurring events.

For the same reason, one does not have to prod the members of the food industry to prepare for serious diseases that can be caused through food poisoning and contamination. What one does have to do is to prod the members

of one industry to look at the kinds of crises that can occur in others and to ask them what they might learn from one another.

One of the best vehicles for accomplishing the preceding are Crisis Forums. A number of CM consulting firms have made it a regular part of their business to bring together members of distinctly different industries so that the chances of their learning from one another are increased. In this way, they help to partner "successful relationships" between members of very different industries.

For instance, one of the more "happy marriages" resulting from one of these forums was the following: An electronics company decided to view itself as being in the food business. This was not as far-fetched as it might seem at first glance. Since "bugs" and other contaminants were a potential source of problems in manufacturing high quality electronic components, it was not a big leap to view computer bugs as literally being microbes. In addition, since many of the components in its products involved the growing of crystals, the leap was not as great. In other words, the metaphors of "growing food" and "growing bugs" were applicable to its business.

This led the company to view quality control as a matter of eliminating "latent bugs or living microbes" that could foster and "grow inside" its products and manufacturing systems and thereby "literally contaminate or poison" its products. Thus, instead of viewing quality primarily as a matter of eliminating hardware, manufacturing errors and malfunctions, quality was now viewed as a task of eliminating "potential diseases."

As a result, the company hired a medical specialist in infectious diseases to come into their organization and to scrutinize their entire systems and products from this distinctive, if not unusual, standpoint. This helped the members of the top executive team to focus explicitly on various "diseases or pathogens" that could be "injected into" the system either by overt criminal acts, breakdowns in procedures, or through faulty management. To counter these, a team was set up to look into possible "inoculations" that could be used as "preventative health measures" to protect, and even to improve, the system.

For example, a common frequently occurring pathogen in the system was the constant pressure by top management to get products out the door. Even thought quality control was taken extremely seriously, over time, there were subtle and not so subtle pressures developing in the culture to get its products out the door so that it could compete more effectively with competitors. With the help of the medical specialist, this behavior was now seen as a possible "pathogen" in the system. Thus, the "inoculation" in this case consisted of the setting up of appropriate reward systems that would help people resist the "disease" or pressure to get products prematurely into the marketplace. Serious thought was also given to various "quarantine measures." That is, products would be "quarantined" unless they passed new rigorous, inspection procedures.

Creative thinking was also given to setting up "new metrics," i.e., new scales that would explicitly measure the amount of money saved due to the non-occurrence of crises. In other words, the organization took serious steps to measure how much was added to its bottom line by preventing crises. It did this

by comparing its record of defects and returned products with other members in its industry.

Another company took the infectious disease metaphor even further. It asked itself the provocative questions, “Suppose we view each of the families or Types of crises in Table 1 as different types of diseases? What would the result be if we did this?” In response to its own questions, it viewed the particular category of Informational crises as “patient diagnostic information.” Thus, an informational crisis would be getting both the wrong diagnostic information from a patient and also making the wrong diagnosis. The relationship to its business was getting the wrong informational design specs for a product. In turn, this also led this same company to view Informational crises as rare or exotic diseases that would escape detection by ordinary means.

In a similar manner, it went through every family in Table 1 and assigned to it a unique category associated with a different type of disease. For instance, Informational crises can also be viewed as “breakdowns of the body to process biological, chemical, and genetic information.” This could be due either to defects in the brain, i.e., the company’s informational systems, or any of the body’s immune “information centers.”

Furthermore, the company appointed a “medical champion” for each of the families. The champion’s role was to take charge of each family and to develop multiple scenarios and strategies for dealing with it, especially the establishment of early warning signals. Thus, the various families were viewed in turn as the “heart,” the “lungs,” the “lifeblood,” of the organization. Next, a “Chief

Medical Examiner" was appointed to coordinate general, overall strategies for insuring the "health" of the entire organization. To put it mildly, this is a prominent example of truly thinking outside of the box.

Construct a "Wheel" of Crises

Mitroff has also used the following brainstorming exercise in helping organizations to think creatively about the unthinkable, and especially, Abnormal Accidents or crises. For instance, the names of each of the different families or Types of crises are put on the circumference of a large wheel containing a pin in its center. The pin is then spun successively. Every time it lands on a particular family, the name of that Type of crisis is noted. After a minimum of at least three spins, the participants in the exercise are encouraged to come up with the most bizarre, "off the wall" examples of each Type that they can think of. No idea, however bizarre, is excluded, at least not initially. The participants are typical from the upper most top and middle management levels of a company.

The members are also encouraged to "slam together" as "violently as they can" each of the various families. In this way, they are encouraged to increase the magnitude or the intensity of each new combination as much as possible. Using this method, a few workshops were able to come extremely close to 9/11 scenarios before it happened. They accomplished this by combining highjackings and car bombings.

Previous car bombing attempts have been mainly confined to conventional vehicles. Previous attempts at highjackings have been largely

confined to airplanes that for the most part were successfully prevented from taking off. However, by “violently slamming” these two types together and by “dramatically increasing the magnitude and the intensity of their combination,” one very easily gets to 9/11 scenarios.

One company debated two dramatically different ways of implementing the results. The first way they considered was a version of Risk Analysis. The company ranked their various facilities around the world from the most to the least vulnerable with regard to terrorist attacks. They estimated the probabilities with which their various locations could be subject to terrorism. In addition, they also estimating the consequences in dollars that would result if this occurred. Then, by multiplying the probability of the occurrence of a terrorist times the consequences, they were able to arrive at the Expected Value of terrorist acts at their facilities around the globe.

The other approach that the company debated was that of randomly selecting sites around the world to prepare against terrorism attacks. The reasoning here was that if the company could apply Risk Analysis to its various locations, then so could potential terrorists. They reasoned that one of the prime characteristics of terrorists is not only their ability to turn conventional assumptions on their head, but to “out think” their potential victims.

As a consequence, the company decided to employ a mixed strategy. It decided to spend 50% of its resources for preparing for terrorism on the sites that it deemed the most vulnerable. The remaining 50% was to be distributed at sites selected at random. To begin the effort, it decided to make a total

expenditure of $5 million for the coming year. $5 million was literally a tiny fraction of the hundreds of billions of dollars in annual sales and assets. It was also a fraction of the cost of major crises such as the $500 million dollars that was incurred by both Ford and Firestone.

Hire People from Different Professions to Scrutinize Your Organization

More than one organization with whom Mitroff has consulted has hired investigative reporters to write the most damaging stories that he or she could concoct based on what they were able to uncover from company files. The reporters also accomplished this merely by examining current company practices, its past history, and by interviewing disgruntled employees. As a result, the reporters were able to prepare mock-ups of hypothetical newspapers that presented the organizations in the worst possible light.

Other organizations have hired movie producers to make a short 20-second video that could be aired on 60 Minutes, 20/20, or CNN, showing the organization in the worst possible light. Because of their intense drama, these "vehicles" were able to break through the considerable denial held by top executives that "such things absolutely couldn't happen to us."

The thing that all of these scenarios have in common is that the organization knew about potential problems long before they actually resulted in a major crisis. In addition, there was a strong trail of early warning signals, often in the form of memos, that were covered up and held under tight cover. The

assumption by the Chief Legal Counsel is that such memos could and would be protected. In virtually every case, they were dead wrong.

Concluding Remarks

In today's world, the potential for all kinds of crises has not only been increasing steadily, but it would seem, almost without limit. In addition, new examples of each of the various types in each of the families, both Normal and Abnormal, are emerging constantly. As a result, there are no absolute, sure-fire ways or guarantees to prevent all crises from occurring.

Nonetheless, while the particular forms that the various Types can assume are virtually limitless, the general categories or families are relatively stable. By itself, this fact offers more than a mere modicum of hope.

If organizations can learn to make thinking about the unthinkable part of, and integrated with, their everyday business operations, then they can improve substantially their chances of not only surviving a major crisis, but actually prospering from them.

To accomplish this, new corporate functions and mechanisms are needed. For instance, we believe that a new corporate function is called for, that of the Chief Crisis Officer or COO. The COO is responsible for coordinating all of the crisis plans and procedures of the company. The COO will also be the head of the Crisis Learning and Signal Detection Center or SLSDC.

The purpose of the CLSDC is the assemble the patterns from past crises and near misses. For example, what were the causes of past crises?

Why did they occur? When? Could they have been prevented? Are there any common patterns that cut across diverse Types of crises and hence reveal dangerous forces that are at work in the culture of an organization?

A critical task of the CLSDC is also to pick up, to amplify, to bring together into an integrated whole, and to disseminate to the right persons the diverse, and often separate, early warning signals that precede every crisis. For instance, since products must function in widely varying weather climates around the globe, do products fail at faster rates in different temperature zones?

In the end, the critical difference is between those organizations that are Crisis Prepared and those that are Crisis Prone. Crisis Prepared organizations not only view CM as a competitive advantage, but practice it as such.

Figure 1:
TIMELINE OF MAJOR CRISES