It seems impossible to plan for crises you can’t even imagine. But a set of surprisingly simple tools can demolish mental barriers—and help managers think about the unthinkable.

Preparing for Evil

by Ian I. Mitroff and Murat C. Alpaslan

Over the last 19 months, the sheer spate and scope of crisis, from terrorism to Tyco, has forced firms to reevaluate the state of their crisis preparedness. Businesses that had crisis management plans in place reviewed and reinforced them. They analyzed the causes of each disaster and near disaster they had faced in the last five to ten years, calculated the costs, and evaluated the risk of recurrence. But despite doing it by the book, many companies have found that a sense of security eludes them still.

Quite simply, the tenets of traditional crisis management are not serving us well anymore. Something critical is missing: the ability to think comprehensively about crises. Most companies develop and refine plans to improve the way they handle emergencies of the kind they have confronted in the past. But they face a bigger threat from calamities they have never faced or, worse, from threats they cannot even imagine they would ever have to cope with. As a result, they are, essentially, fighting new wars with old strategies.

Crisis Prepared or Crisis Prone?

The problem is widespread. For the past two decades, the University of Southern California’s Center for Crisis Management monitored the crisis readiness of the Fortune 500 companies, primarily by conducting on-site crisis audits of a wide variety of organizations, public as well as private, and through periodic surveys. We believe it’s possible to draw important general conclusions from our 20-year study.

We grouped the companies in our study into two broad categories: crisis
prepared (or proactive) and crisis prone (or reactive). Crisis prone businesses prepare to handle only the types of calamities they’ve already suffered, and not even all of those. Crisis-prepared companies develop plans to handle a larger number and wider variety of emergencies than they have faced in the past. The distinction is not particularly subtle, but its implications are important.

For most of the two decades, crisis-prepared companies were in a small minority: between 5% and 25% of the Fortune 500 companies at most. In other words, at best, 75% of companies are not equipped to manage an unfamiliar crisis. At worst, 95% are unprepared, which, of course, is extremely worrying.

It’s also unfortunate because our research further shows that being prepared for crises pays off in several ways. First, preparedness reduces the number of calamities companies have to grapple with. Between 1998 and 2001, the average crisis-prepared company reported that it had coped with 21 emergencies; those that were less prepared faced 33 crises. Clearly, planning for trouble reduces its incidence, just as putting a lock on a door cuts down on burglaries, even though it does not eliminate them entirely.

Second, crisis-prepared companies stay in business longer. According to the 2002 survey, proactive companies had been around for 83 years on average—24% longer than reactive companies, whose average life span was 67 years.

Third, the crisis prepared fare better in financial terms than the crisis prone. In 2001, for instance, the average return on assets of proactive companies was 6%—double the average return the crisis prone group posted that year. We don’t attribute the superior performance only to better crisis management, but there’s no doubt that proactive companies incur lower crisis-related costs. And a crisis-prepared company is likely to be a better steward of its assets in other areas as well, like financial risk management.

Finally, preparedness affects corporate reputations. In 2001, for instance, the proactive companies notched up an average score of 6.2 points on Fortune’s eight-point scale ranking the most admired companies in America, whereas the reactive companies averaged only 5.6 points.

That isn’t entirely surprising because the two groups’ approach to crisis management appears to be fundamentally different. Our research shows that crisis-prepared companies believe no harm should come even to one person when a crisis erupts. They understand that the effects of a disaster cannot be predicted or controlled, so it’s more important to prevent crises than to contain them. The crisis prone, by contrast, assume that it’s enough if they secure the greatest good for the greatest number, so they seek to invest in crisis readiness only to the extent that it is cost-effective. That leads them to presume, wrongly, that the consequences of a crisis can be predicted and the possible costs can be weighed against the expenses of preventing it.

Ironically, the businesslike approach of weighing costs and benefits turns out to be more costly; as we have shown, the crisis-prepared suffer fewer crises, recover faster, and are more profitable than the cost conscious, crisis prone businesses.

The New Crisis

Being crisis prepared doesn’t require companies to plan for every disaster that could conceivably affect them. That is neither necessary nor possible. But there are ways in which companies can think broadly about the full range of problems they might encounter and create strategies to lower their vulnerability. We’ve studied the disasters faced and the plans drawn up by more than 150 businesses all over the world. We’ve also conducted crisis management audits in more than 60 multinational corporations, government agencies, and nongovernmental organizations. Our research suggests that proactive companies distinguish between three general forms of misfortune.

The first are natural accidents, like fires or earthquakes. For the most part, companies know how to prepare for these crises and can defend against them using risk management techniques such as safety planning and insurance. The second kind is what’s called normal accidents. The term was coined by the sociologist Charles Perrow. In his 1984 book, _Normal Accidents: Living with High-Risk Technologies_, Perrow pointed out that technologies have become so complex that the potential for breakdowns is literally built into them. In fact, industrial disasters like Three Mile Island, Chernobyl, Bhopal, and Exxon Valdez were not random aberrations but normal system-overload and malfunction problems. Preparing for them is challenging, but crisis-prepared companies cope, for example, by getting designers, operators, and maintenance managers of complex systems together regularly to compare notes. If the conditions the operators are experiencing aren’t in line with the designers’ assumptions, then a normal accident is in the offing.

Ian I. Mitroff is the Harold Quinton Distinguished Professor of Business Policy at the Marshall School of Business, the director of the Center for Strategic Public Relations, and a professor of journalism at the Annenberg School for Communication at the University of Southern California in Los Angeles. He is the author of 22 books, including the forthcoming Crisis Leadership: Planning for the Unthinkable (John Wiley, 2003). Murat C. Alpaslan recently completed his doctoral degree at the Marshall School.

If they are to cope with abnormal crises, companies must learn to see—as their enemies do—skyscrapers as vertical coffins and aircraft as flying bombs, ugly and horrifying though the prospect may be.
Most important, proactive companies worry about a third category of calamity—what we call abnormal (that is, intentional) accidents, which are the result of deliberate evil actions such as bombings, kidnappings, and cyberattacks. Companies, particularly those that operate in developing countries, have always lived with the possibility of sabotage, whether by employees or outsiders. But the danger has never been greater than it is today because of global terrorism, which has landed workplaces all over the world in the middle of a war zone.

In fact, the number of abnormal accidents has risen sharply in the past ten years. We constructed a time line of the major crises that have occurred since 1979 (see the exhibit “A Time Line of Major Crises”). Although the classification is not exact, and our time line is by no means exhaustive, our analysis suggests that there were as many abnormal crises in that period as normal ones. While normal crises were more prevalent in the 1980s, abnormal accidents dominated the 1990s. Moreover, the impact of some of those deliberate events rivaled that of natural disasters.

It isn’t, of course, as easy to prepare for abnormal accidents as it is for normal ones. Most people find it difficult and distasteful to imagine that fellow humans would want to destroy businesses deliberately, sometimes with the collusion of employees, and would be willing to kill themselves in the process. Making such assumptions destroys our deeply held beliefs about people, society, and business, and there is a great deal of denial and disavowal in companies about the size and scope of abnormal accidents. That is stupid behavior by nonstupid people, as psychologists like Albert Ellis would describe it. But irrational beliefs and self-defeating behaviors are common while planning for crises. Even a year after the World Trade Center was brought down, most executives we spoke to had not considered the possibility of a similar attack on their offices or factories. If they are to cope with abnormal crises, companies must learn to see—as their enemies do—skyscrapers as vertical coffins and aircraft as flying bombs, ugly and horrifying though the prospect may be.

Creative Demolition: A Crisis Tool Kit

It is precisely for that reason that companies need to develop special skills to come to grips with abnormal accidents. In the following pages, we will describe how some businesses have learned to
Some companies prepare effectively for abnormal crises by thinking about them at random.

list on it all the crisis families that a company can face. (See the exhibit “The Wheel of Crises.”) Executives take turns spinning the wheel; when the pin stops, they discuss all the normal and abnormal crises of that particular kind they can imagine. We don’t exclude any possibility, however bizarre, because each one helps overturn the executives’ fundamental belief that they already know what crises the company could face.

In the next stage of this version of Russian roulette, participants club together two abnormal crises to create a more improbable combination crisis. That increases the magnitude of the peril and compels executives to accept that abnormal disasters often happen on a very large scale. It also helps them link crises they never thought applied to their company or industry. Chillingly, executives at more than one Fortune 500 company we worked with back in 2000 combined a car bomb and an aircraft hijacking to come up with the threat of a “flying bomb” — distressingly close to the World Trade Center attack.

The random-selection model can also be the basis of a rational budgeting strategy for an illogical world. Each year, smart companies focus their resources and attention on a few of their facilities picked at random, just as airlines carry out detailed security checks on a few passengers for each flight. That reduces the probability of an attack on the entire organization even as it allows the business to migrate gradually to a higher level of crisis readiness. After one global corporation evaluated the vulnerability of its more than 100 facilities to terrorist strikes, for instance, it realized that it

A Time Line of Major Crises

The number of accidental crises, whether natural or man-made (normal), are increasingly being overshadowed by abnormal (or deliberately precipitated) crises. Yet most companies remain unprepared for any kind of calamity.
could not afford to immediately upgrade the security and crisis response levels at all of them. However, the company did not allocate its annual crisis management budget of $5 million in proportion to the weakness of each site. Instead, it announced that half would be spent on sites the company had randomly selected and the other half on the most vulnerable ones. In the process, the company created a stronger deterrent without increasing budgets.

**Internal Assassins.** Many of the crisis-prepared companies we worked with rely on their people, who know the organization best, to develop abnormal situations that they should prepare for. However, employees need to be trained to imagine the worst, since they usually apply their knowledge of the company for its benefit, not its destruction. Special techniques like role-playing can get them to think (temporarily) like villains.

We often ask small groups of top or middle-level executives to imagine themselves to be internal assassins or internal terrorists. That frees them to suspend their rationality and moral codes and allows them to use their intimate knowledge of the company's products, procedures, and systems to cook up ways to destroy it, either from the inside or the outside. In one large U.S. company we worked with, for example, we designated a group of ten senior executives as internal assassins. We walked the group through several of the company's manufacturing facilities, both during the working day and after office hours. As the executives began to see the plants through terrorist eyes, they almost reluctantly started pointing out where they would cause the most damage, how they could do so, and the entry and escape routes they would use. The scenarios were frightening both because they exposed weaknesses in the system and because they were plausible.

The internal assassin technique can often change the organization's attitude to crisis. Take the case of a $1 billion U.S. medical insurance company, which used the exercise to work out if financial fraud could force it into bankruptcy, as Barings, the British merchant bank, was in 1995. It set up three teams, each consisting of eight senior executives. Team A was asked to devise swindles that employees could carry out; Team B, fiddles that outsiders could mount; and Team C, schemes that crooked outsiders and employees could work in collusion. Much to everyone's surprise and...
embarrassment, all three teams came up with ingenious scams that the organization would not have been able to detect.

The insurance company immediately constituted three counterassassin teams to develop systems to prevent or detect the swindles. After several months, these groups independently concluded that the company was most vulnerable to one fundamental problem. If a scamster was patient, he could accumulate a fortune by siphoning off small amounts of money over long periods of time no matter what scheme he used. Consequently, the company lowered detection thresholds across the organization. Managers modified computer systems to flag suspicious transactions, however small they might be, and instituted auditing procedures to examine small payouts as closely as large ones. By looking at its vulnerabilities systematically, the bank was able to close the door on an entire category of threats all at once.

**Mixed Metaphors.** The majority of crisis-prepared companies regularly send executives to crisis forums, where companies from diverse industries discuss crisis planning. But they don't stop at that. They also rigorously apply the metaphors and lexicons of other industries to examine themselves from unusual perspectives and learn from the scenarios that other companies have prepared for. For instance, banks may be equipped to handle cyberattacks because computer crime is easy to imagine in the context of the financial services industry. But they may be less likely to think about explosions, which would spring immediately to the minds of executives at, say, chemical companies.

When firms look at crises that occur outside their own industry, they realize how vulnerable they are. Take the case of a large U.S. electronics manufacturer that chose to envision itself in the food industry. If it were making food products, the company felt, its quality assurance objective would no longer be the reduction of hardware defects. It would be the elimination of latent bugs and microbes that were festering inside products and polluting them. That difference so intrigued executives that they hired an infectious disease specialist to assess how the company could prevent pathogens from contaminating their production systems and infecting their products. During the rather unusual scrutiny, the company learned that pathogens could be deliberately injected into their products, turning them into Trojan horses that transmitted disease rather than well-being—a possibility that food and drug companies routinely envision, but not manufacturers of electronics.

The alarmed giant decided to come up with ways to prevent such crises. One pathogen it identified was the possibility that a disgruntled employee or supplier would deliberately introduce faulty components into a product. As an inoculation, the company stipulated that executives must determine if product failures had been deliberately caused, once customers reported a certain number of them. In addition, products that
had not been shipped would be quarantined until the inoculation had been administered. Applying the food industry’s metaphors helped the electronics giant come to terms with the fact that product tampering was a threat it might have to cope with.

**Spy Games.** Proactive companies aren’t shy about bringing in outsiders to test their vulnerability to abnormal crises. They realize that sometimes employees possess too much knowledge about the organization or are too steeped in everyday operations to adopt radically different perspectives. The creative use of impartial experts helps companies overcome both the “That doesn’t happen here!” and the “That can’t happen!” syndromes.

Smart companies hire professionals like investigative journalists, lawyers, and consumer affairs experts to stage hypothetical assaults on them. Such simulations expose weaknesses and test responses at the same time. Some companies we consulted with commissioned journalists to write investigative stories or produce 20-second videos that attacked products, top executives, or reputations. The writers based their articles on actual attacks by disgruntled employees or business rivals. The intense drama of the exercises helped executives break through their disbelief and accept that they might well have to tackle such crises someday.

Other organizations ask journalists to report on their crisis prevention plans or their level of security consciousness. That helps companies almost as much as internal crisis management audits do. Here’s what one reporter hired by a U.S. company to snoop around one of its major facilities found: “A large number of files containing confidential information, sometimes dating back a decade or more, have been dumped in a basement in the main building. But there are few security checks in place. Any employee—and almost any visitor—could get at them if he or she wanted to. In fact, I was offered a random assortment of files for a small sum of money.” No one in the company had realized how vulnerable those files were: Two months later, a disgruntled employee was caught trying to access some of the documents.

The criminal mind-set is so different from most people’s that executives can often figure it out only by bringing it inside the organization. Banks hire former robbers to test security procedures. Casinos in Las Vegas use professional gamblers to fight cardsharps. Insurance companies recruit reformed scammers to detect fraud. Many companies have used professional hackers to probe the safety of computer networks. The results are startling. For instance, when a crisis center has three responsibilities. First, it designs the company’s crisis portfolio, which consists of at least one possibility from each crisis family, and draws up prevention and response plans for them. Some centers have appointed champions for each type of crisis who help develop scenarios and strategies just for that type of emergency. The crisis center also prepares for the possibility that one calamity might trigger another or that more than one crisis might erupt simultaneously—scenarios that are becoming increasingly common.

Proactive companies aren’t shy about bringing in outsiders to test their vulnerability to abnormal crises.

Ace-hacker-turned-security-consultant Kevin Mitnick identified what made companies most susceptible to hacking; it wasn’t software or systems (see “Are You the Weak Link?” in the Forethought section of this issue). It was honest, unwitting employees—hardly what most information technology managers think of as a major threat to computer networks.

**Establishing a Crisis Center**

Many executives at even well-managed companies secretly believe that they can work their way out of a crisis when the time comes without having a plan beforehand. As a result, they treat crisis preparation as a less-than-useful scenario-planning exercise that, if it must, can be conducted sporadically. That attitude won’t change until companies create organizational mechanisms that make crisis management a priority. Crisis planning has usually been regarded as part of risk management, which is handled by the controller’s office. Or it’s been relegated as a lesser responsibility to the human resources or an administrative department. Either way, it ends up being less than half a job for someone for two or three levels below the CEO. To elevate the function, proactive companies have created a crisis management office or crisis center, whose head reports to the CEO, COO, or CIO.

Second, the crisis center stays alert for the signals that inevitably precede a crisis, amplifies them, and distributes warnings to the right executives in the company. By integrating signals coming from, say, different parts of the world, organizations can often detect problems before they blow up. Ford might have averted the Firestone tire crisis in 2000, for example, if it had paid attention to reports of its tires coming apart in Saudi Arabia and Venezuela. Instead, it wasn’t until after the crisis erupted in the United States that Ford put together a 500-person task force to see if it faced similar problems elsewhere.

Finally, it is the crisis center’s responsibility to go beyond paper plans to develop real crisis capabilities. It conducts regular audits and training exercises, installs mechanisms to contain crises, and develops programs to help executives communicate effectively with internal and external stakeholders during a crisis. It also identifies or sets up alternate work sites in case the company’s offices and plants are destroyed. That isn’t as far fetched as it once seemed for, as author Salman Rushdie said as long ago as November 1990, “One of the extraordinary things about human events is that the unthinkable becomes thinkable.”

Reprint R0304J; HBR OnPoint 3388
To order, see page 125.