The following is a highlighted summary of the book, Crisis Management for Corporate Self-Defense, *published by New York AMACOM Books. The statements below are key points of the book as determined by James Altfeld and have been made available at no charge to the user.*

Crisis Management for Corporate Self-Defense

By

Steven Albrecht

Have we seen public relations nightmares with moral and political overtones?
Do we have employees who destroy, alter, or steal data, assets, or inventory?
Do we have armed and disturbed employees killing their co-workers?
Have we seen the sudden death of a CEO or other top company leaders?
Can disasters like floods, earthquakes, hurricanes, and fires put an unprepared form nearly or completely out of business?
Is sexual harassment still an issue in our workplaces?

Whether the crisis is brought about through fate, misfortune, negligence, or error, it can be hard to keep the press, lawyers, toxic employees, outside agitators, and just plain bad management from messing up corporate works.

If it happens in life, it can happen at work,

> People who say of their company, "We don't have a drug problem here," are not paying attention to the world around them. If 10 percent of Americans are challenged by depression, then 10 percent of *American workers* are challenged by depression. If family abuse is a problem in society, with women and children more likely to be victimized by a family member than in the worst alley of the worst ghetto, then it's also a problem in the workplace. To believe that you have a controlled environment, a campus of sort, where you decide who comes in and who doesn't and where nothing bad ever happens, is a mistake.

A business-basis crisis is an event-specific episode that can make or break you, depending upon the size of your company, the number of people you employ, the products and services you sell, and the resources of people, assets, and money you can aim at the problem.

What could be a full-blown “crisis” for one company-- i.e. involving the potential or actual loss of products, data, assets, goodwill, personnel, or money-- might have little impact on another firm with more resources and a better plan to cope with the problem.

(p.11)

CEO or other top executive apathy tends to manifest itself in several ways:

- “Those kinds of things don’t happen around here, at least not on *my* watch.”
- “Hey, I’m not running a babysitting service here, I expect my employees to act like adults, do their work, and leave their off-the-job problems at home.”
- “We pay our managers and supervisors good money to take care of that stuff. It’s their responsibility to fix things. And if they don’t, the fault lies with them, not us.”
- Employee problems are the responsibility of the HRD, personnel, employee assistance, or security departments. We don’t deal with those kinds of things at the senior management level.”
- We tend to fly by the seats of our pants around here. If something does come up, we handle it then.”
- “Those things happen at other companies. We’ve never had that kind of problem here, so we don’t waste time worrying about it.”

Of all the executive excuses, the most dangerous is the one that goes, “It could never happen here.”

What has happened or has not happened in the past is not an accurate indicator of the future.

“When the phone rings past 10:00 p.m., its rarely good news.”
As one veteran public relations executive puts it, “When the worst hits the fan and your company is suddenly faced with some kind of disaster, it’s never on a Wednesday in the middle of the afternoon. When the phone rings with bad news, it’s always a Sunday, on Easter, during a snowstorm, when your CEO and the number-two guy are on a plane for the next five hours and completely unavailable.”

Writing your “Bug List”

A Bug List should cover major problem areas-- potential issues, relation to liability with your products, services, employees, or customers, or current risk-related events that require immediate or very-near-future solutions.

When you look across the broad landscape that is your company, what is it that troubles you most? Which current or potential problems keep you awake at night?

Potential Crisis Problems, Risks, and Events

- What problems may occur with out products that will require special management skills?
- What problems may occur with our services that will require special management skills?
- What problems may occur with our employees that will require special management skills?
- What problems may occur with our customers that will require special management skills?
- What problems may occur with outside vendors or business partners that will require special management skills?
- What kinds of preexisting plans do we already have in place to manage one or more of these events?
- Who is in charge of managing out response to one or more of these events? Is it me? Is it the people above me or below me? Do we have a team of people trained to react to a variety of problems?
- What kind of training needs to accompany our management responses to one or more of these events?
- Is our company organized around a response-based chain of command, so that each person knows his or her role?
- Will we be able to manage our image properly, protect our human and company assets, and continue to serve our customers should one or more of the events occur?

It is important to recognize that during and following any significant event (not necessarily relation to violence) the *victims* don't think clearly, and since the *employer* is as much a victim as the *employee*, by proxy, the *organization* doesn't think well either. In other words, the company's coping mechanism is suddenly on the fritz.

What this means is that, once they're embroiled in a significant problem, companies often make things worse for themselves, not because they mean to, but because the people at the top, who must make important decisions during and following critical incidents, can get trapped in the victim mode as well, and thus fail to respond properly.

In times of great stress, we revert back to what we know, and more importantly, how we have been trained and conditioned to respond.

If you have some idea of what to do first, next and last during any significant event, you will fare better than your counterparts or competitors, who, when faced with similar problems, will let indecisiveness, ignorance, or just plain wrong influences affect their behaviors, reactions, and responses.

Having a plan for responding to a significant business problem or true crisis and then never needing it is life paying on a life insurance policy when you're in perfect health; you just never know what the future holds.

The fire at the manufacturing plant was due to friction caused by a large inventory rubbing up against an insurance policy.

The "toxic" manager or employee who goes around the company destroying its physical or psychological assets may have an agenda that is personal, secret, and volatile.

The disgruntled customer who races to the first lawyer he can find who will take his case may be more interested in a nuisance settlement from you than real justice.

The activists who protest at your doorsteps will have a very vocal agenda-- publicity for their case, the need to express their anger over what they feel is corporate greed or apathy, and the desire to create change through the infliction of real pain or other media-generated discomfort.

Visible or not, the need for recognition, money or a pound of flesh drives many people, either alone or in groups, to go after our institutions: government, politics, school, law enforcement, the courts, the media-- and of course, business.

"Was this problem created by people, an accident, or an event related to or unrelated to our current work with our products, services, or customers?"

If the cause of your current problem is associated with some form of human intervention-- a lawsuit, a strike, a security problem, a boycott, a protest, or an attempt to bring your firm into the media limelight, you should ask another important question: "If outside people or disgruntled employees are at the root of this problem, what is their agenda?"

"Will out various responses to this problem advance, hinder, or have no effect on their agendas? And what will our responses do to further out own agendas as a company."

A Lawsuit

The primary goal of the plaintiff may be money-- your money. The secondary goal, however, may be exposure, publicity, media attention, or the desire to stick a thumb into your collective eye. Money may not be the only issue if their goal is to try to embarrass or humiliate your firm in a courtroom.

Trying your case in the newspapers may not pay dividends either, but there is much to be gained by taking a defensive stance that says, "We will fight for our rights now, not two years from now when the case finally goes to trial."

If you can determine what the other side's agenda is at the preliminary stages of any suit, you can set up a defense based on early action rather then taking the usual "no comment, we'll wait for a court date" stance that so many companies seem to choose as their only way out.

Agendas become complicated in union struggles. Your efforts to enhance your position in the public eye by stating "We want everyone back on the job and we want to get out firm back to full productivity," can do more than simply stating, "There are no new talks scheduled."

Few firms want to air their dirty laundry in public. Company leaders reason that any apparent breach of security-- e.g., a theft ring, violence, vandalism or sabotage, lost or stolen information, etc.-- will make them look weak or out of control.

The company that admits that its computer files were "hacked" and then publicizes new antihacking, antivirus security measures tells other people, "We're concerned about this new crime and we want to stop it from harming us ever again."

With domestic violence in the workplace becoming a viable issue, some firms have publicized their involvement in awareness and prevention campaigns.

A Boycott

Agenda
"Give us as much news coverage as possible while we engage in this behavior."
The boycotts set can be very damaging to your reputation.
Unlike lawsuits, it sometimes pays to admit your faults, settle the dispute, and move on.

A Protest

Protesters want media coverage first and foremost. Then they want to feel the satisfaction of having disrupted your business operations and activities for an hour, a day, a week, a month, or a year.

The best way to handle their agenda is to ignore it.

The best way to have the media on your side is to have them on your side in the first place. The agenda of the mudslinger is to make your firm look disreputable, dangerous, or even hazardous. If you help the media see that your reputation is sterling, your products and services are top quality, and your policies and procedures for handling your employees and customers are fair and equitable, you'll be way ahead of the mudslingers.

Where the disgruntled employee tells all who will listen, "I hate this place and it's somebody's, anybody's fault but mine, "the entitled employee says, "I *deserve* this and I *deserve* that… I'm entitled to those things and I want them. If I don't get them, I might quit, sure, lash out at you, or just take what I want."

For some people, the old approach-- pull yourself up by your bootstraps and you can make a better life at home and at work-- is fast being replaced by the new work ethic that says, "I'm underpaid, underappreciated, and underrespected. This company doesn't demonstrate any loyalty to me so I don't feel any loyalty back. As far as I'm concerned, thanks to downsizing and this economy, I'm two weeks or less away from my next job anyway."

Employees believe that their company owes them more than a paycheck.

(p.24)
"Because we haven't had a raise in seven years!"

Social proof to describe the use of certain perceived social behaviors as justification for their own, similar behaviors-- i.e. “It’s being done by others around me, so it must be acceptable.”

20 percent of your employees will cause 80 percent of your problems.

An employee of a neon sign shop was fired for being late nearly every day of his 10 years on the job. He filed a lawsuit against the shop, saying that his tardiness and absenteeism was due to a subconscious fear of being on time. The shop owner lost and was forced to pay a large award to the man.

A gas station owner fired a mechanic for working while drunk and smoking marijuana on the job. The terminated employee somehow convinced a state labor board that his drug and alcohol abuse was stress- and job-related. The owner ended up paying $3,000 for the mechanic’s stint in a chemical dependency center.

A union employee brought a gun to his job, pointed it at a co-worker, and pulled the trigger. The gun misfired and the man was later overpowered by other employees. He was later found to have a history of mental illness and substance abuse. After completing a series of treatment programs, the man came back to work and was given limited-duty jobs because his original position had been phased out.

When he was let go because he was thought to be a safety risk, a union arbitrator ruled that he should be allowed to come back to work because the company was legally obligated under the Americans with Disabilities Act to help him treat his substance abuse, violence, and psychological problems.

In toxic culture, jobs are designed to create as much stress in the employees as possible; policies and procedures are written and enforced to punish the employees for their errors rather than reward them for the successes; and the employees are spoken *at* and treated as if they are the root cause of what’s wrong in the company. Issues like employee participation, mentoring, empowerment, and feedback are thought to be too “soft” to be addressed by top management.

The fault in the toxic company lies not so much with its people, but with its culture.

(p.32)
Once the incident was resolved, Tom McNally, president of Ross Products Division, published an open letter to his customers.

> As the makers of Similac, America’s leading infant formula, we at the Ross Products Division of Abbott Laboratories take safety and quality seriously. Our ultimate customers-- the babies of California, the U.S. and the world-- are too important to take any chances. That’s why we perform nearly 2,000 tests to assure the quality of every batch of Similac we make. We value the trust that you’ve given us for many years.

Individuals recently took advantage of that trust by manufacturing and selling California retailers a powdered substance in counterfeit Similac cans. We worked with the U.S. Food & Drug Administration (FDA) throughout this episode to let the public know about this crime, and to protect our customers from this fake product.

We are very happy to acknowledge that the FDA has apprehended one of the individuals believed to be responsible, and seized the manufacturing operations used in this illegal activity. The FDA reports that all known counterfeit product has been removed from retail stores. Parents can continue to use Similac products with full confidence.

We have many people to thank for this successful outcome. First is the FDA, whose outstanding efforts brought about a swift conclusion. Second, are the many committed Abbott employees who worked around the clock, answering customer questions assisting the FDA.

Finally, and most importantly, we want to thank you, our customer, for your continued trust and confidence in Similac.

- It gives lots of information to all who read it: current customers of Similac; future customers; retailers, distributors, business partners, and even competitors.
- The tone is upbeat, reassuring, thankful, and positive. It conveys no evidence of malice toward the perpetrators (which might distract customers from the real message). More important, it doesn't seek to fix the blame anywhere else but where it belongs.
- The letter is careful not to go overboard in its sense of outrage at the people who attempted this crime. There is no whining, finger-pointing, no sense that the company did not take complete control of the incident after it first surfaced. Readers of the letter can infer from its existence that the company was upset by the problem. But the organization carefully focuses the attention on the positive outcomes rather than on the negative ones.
- It makes significant, specific mention of its production and testing procedures as a way to demonstrate the company's constant and ongoing commitment to product quality control.
- It severs to distance the company and its product from the acts of the culprits and their counterfeit.
- It delivers plenty of praise exactly where it belongs: to FDA investigators; to Abbott Labs employees, who from this reading appear to have worked extra hard to protect the company's name, reputation, and goodwill with their customers; and to its customers for sticking with the company through this tough time.

(p.35)

Let's Wait to Comment:

Foodmakers Early Media Response

Not only was the company caught off guard by the incident; it was unprepared for the emergency's scope and size. As a result, too much time elapsed before the company took significant steps to change its restaurant operating procedures or its handling of the information given to or uncovered by the media.

About 100 of these franchisees files a class action law suit against the Foodmaker, claiming among other things a $100 million loss due to the problem.

Both sides had attempted to settle their financial differences during meetings between attorneys for the franchisees and Foodmaker, but they failed. In that respect, Foodmaker seemed to view its franchisees as adversaries and not as business partners.

Foodmaker had purchased the meat from Vons and yet, during the heat of the controversy, Von's name was conspicuously absent from much of the media spotlight. Even the fact that the Foodmaker sued Vons, its meat processor, and 10 other companies that provided the bad beef to Jack In the Box, received no more than a short mention in the newspapers.

To say that the *E. coli* bacteria breakout created a huge public relations mess for Foodmaker is like saying the Titanic ran into some difficulty with ice.

It must have been difficult for many of the employees to admit to other people that they worked for a company involved in a tainted-food problem.

Again in hindsight, perhaps if they had not used the wrong temperature for their grills maybe no one would have been poisoned and it wouldn't have been a problem in the first place.

Consider the fact that days passed before the company had publicly announced it had changed its meat-cooking policies. By the time it got around to saying anything, the damage had been done, both to its reputation and to the level of prior consumer confidence.

(p.40)
(In military parlance, this "stop for safety" operation is known as a stand-down.)

- Consider shutting down the operation
- Immediately institute an on-the-spot retraining
- Go to the public and to the media

In times like this-- especially when young kids have died as a result of eating your product-- the CEO or other senior company leader must bear the yoke of responsibility.

No Rebound in Sight:
Foodmaker Jumps Back into Fire

And the beat goes on for Foodmaker. Its 1995 ad campaign heralding the return of its corporate clown's-head logo (literally blown up and destroyed by a bomb in TV commercials in 1980) could not have come at a worse time for them. It features the new Jack (a man in a suit wearing a big clown's head), blowing up the boardroom filled with his current bosses. The message for the commercial was supposed to be "Jack's back." Instead, it brought howls of protest from advertising and consumer groups who believe that anything glorifying bombings-- in this era of workplace violence, the Unabomber, and the attacks on the World Trade Center and the Oklahoma federal building-- is in incredibly poor taste.

The ad was created by Foodmaker and ad king Chiat/Day, who together in a statement said, "We discussed the violent content of the ad and thought few people would take it seriously."

The editors at *TV Guide*, no strangers to tasteless commercials, had this to say about it:

> Jeers to the commercial for the [Jack in the Box} burger chain that showed a mad bomber in a clown costume blowing up the company's board of directors. It was *supposed* to be funny-- the clown himself was blown up in an ad 15 years ago, and this was his comic, "vengeance." Unfortunately, the sport ran during a period when a New Jersey ad exec was killed by a mail bomb, an explosive went off in a New York City subway and terrorists tried to blow up a plane over Paris. Our beef is not [just] with the bad timing, but with the company's reluctance to pull the ad off the box.

By the end of the Foodmaker meat problem, three children had died, several hundred people had gotten extremely sick, and a parent company with a previously long history of success (the first Jack In The Box opened in the early 1960's) had to learn and expensive, painful lesson in how *not* to manage a real crisis event.

Only time and the natural ebb and flow of consumer forgetfulness with help Foodmaker and its Jack in the Box restaurants finally distance themselves from this tragedy. Foodmaker had little choice but to pay the money to the survivors and franchisees and try to move on. As its current financial condition indicates, the recovery will be slow.

In the 1983 movie *Strange Brew*, Dave Thomas and Rick Moranis star as two beer-swilling Canadians known as the McKenzie Brothers. In a classic product-tampering scene, they decided to take a baby mouse, insert it carefully into an empty beer bottle and the feed and care for it for several weeks until its fully grown and now stuck in the bottle, then they pour some beer back into the bottle, drive to their local brewery with the beer-trapped mouse in tow, and demand free beer for life.

Pepsi-Cola found out in early June 1993, when the first reports began to surface in Tacoma, Washington, and New Orleans about syringes found inside cans of Pepsi. By June 23, 1993, more than 50 people from dozens of states had come forward.

(The cans move at extremely high speeds and it would take nothing short of a complete assembly line stoppage to get any item, much less a syringe, into one can.)

Weatherup decided rather than attempt a recall, his company would advise people to put their sodas into glasses before drinking them, at least until they got to the bottom of the so-called "syringe scare."

And while the FDA was announcing that the cases they had investigated were hoaxes, Pepsi and Weatherup continued to work hard to reassure their bottlers, distributors, and consumers that their products were safe, drinkable, and free from anything other than soda water, bubbles, and syrup.

Weatherup knew that the company had so many quality controls, tests, product reviews and samplings, that tempering would be nearly impossible. He was able to convince the public to back his product by letting the media carry his message for him. His efforts and the efforts of his company calmed nervous consumers and swung public confidence back over to Pepsi.

"Our product is safe and we won't recall it." -- from start to finish.

(p.74)

"The only things that evolve by themselves in an organization are disorder, friction, and malperformance." -- Peter Drucker.

The largest area of liability that will cause you the most expensive, costly headaches, begin and end with the very people hired and paid to run various parts of the company: your employees.

With plenty of well-tuned robots, there would be no alcohol abuse on the job, no embezzlement, fraud, cheating or theft. We wouldn't have to worry about employees operating the cash registers without error, driving forklifts without accident, or walking out with copy machines under their coats. We wouldn't have to concern ourselves with the ramifications of violence at work, disability claims based upon fake injury claims, or labor-related lawsuits following just-cause terminations.

Nearly 24 percent of 6,200 respondents from 300 different service, retail and manufacturing firms said they were concerned about such issues as customer courtesy, service problems, safety violations, equal employment opportunity violations, and substance abuse. Nearly 22 percent of the survey participants reported concerns related to the theft of goods, cash, and time from their firms.

Other significant issues ranged from policy and procedure violations to payroll problems, falsification of company documents, labor law violations, unauthorized discounts, sexual and physical harassment, conflicts of interest, kickbacks, theft or release of proprietary information, defrauding customers, vendor theft, and fraud.

Most of the problems that force you into a courtroom are related to the conduct and actions of your employees, whether it's the executives, managers, supervisors, or people on the frontline.

The rules of home and life and work have all changed. Problems with drugs or alcohol, once hushed-up, have now become almost fashionable. Employees are saying to their employers, "I have a drinking problem or drug problem. I've tried to deal with it myself, but I can't Now that *you* know what are *you* going to do about it? What treatment program will you put me in and pay for?"

The employee entitlement syndrome that has affected many organizations has also led to out-of-control problems, such as vandalism, sabotage, rampant theft of goods or data, financially oriented "paper" crimes, domestic violence acted out at the workplace, extortion, intimidation, and other acts and events thought impossible, invisible, or unlikely in the workplace as recently as five years ago.

(p.87)
Calling theft by the popular and vaguely oxymoronic euphemism "internal shrinkage," is like referring to a murder as a "death incident."

Twice as much is stolen from companies by *employees* than by outsiders. Most of your products and inventory leave illegally by the employee exit than by the customer exit.

> *Security is everybody's business. The protection of our people and property starts with your awareness of potential problems, your ability to observe and report security issues to the proper department, and your willingness to be alert. This company belongs to everyone, and the employee who steals from one of us, steals from all of us.*

Whether it comes from hacking into systems for the purpose of wandering around a company's files, sheer vandalism (inserting viruses, erasing files, sabotaging existing files, etc.), or the unauthorized and illegal transfer of money, data or trade secrets, computer crime is a reality.

As G. Green and R.J. Fischer put it in their corporate security book, "Probably no element in business presents a greater potential to wipe out an entire business as quickly and so effectively as the computer.

Opportunistic employees load other workers; computers into the backseats of their cars and never return them; manipulative employees steal their own laptops and the report them stolen; or highly specialized burglars, like those striking in the Silicon Valley, take machines, parts, and those expensive (but easily stolen, stored, and resold) computer chips.

The people who take your proprietary data include current, disgruntled, or past employees; internal sub-contractors, consultants, or vendors; competitors; and other individuals or groups who see what you have on paper on online as valuable.

Much of the fault for this theft of information lies in poorly written and poorly enforces policies and procedures regarding data protection.

Your E-mail, voice-mail, and telephone systems, and your fax, cellular phone, and modem lines are no longer impenetrable.

Consider the fact that a small Texas oil pipe firm lost out on a major contract when a competitor hacked into its private voice-mail lines. After two men assigned to win the contract had left each other messages about their bids and pricing information, their competitors successfully broke into their voice-mail system, extracted the valuable information without their knowledge, and proceeded to underbid the contract enough to win it.

(p.94)

- It offered sexual harassment training to all new employees.
- It offered ongoing sexual harassment training to all employees.

1. Have a strong policy against it, which starts with new employee training, no-tolerance policies, ongoing, in-service training, and a bona fide complaint-gathering system.
2. Follow up on any complaints or charges immediately, including immediate, thorough, and confidential interviews with witnesses, victims, and subject employees.

(p.106)

Most company policies and procedures are designed to handle routines, not uncommon events.

Just as the Federal Aviation Administration has a response team of accident investigators who race at a moment's notice to the scene of every airline crash, so should every organization have its own response team. Those involved must, along with their other regular workday duties, be ready to step in and institute an already-created plan of action for any serious problem that turns the organization on its ear.

Any company that is totally surprised by a serious product, service, image, or employee problem is badly managed.

"The time to look for the water supply cutoff is *before* the pipes have broken, not *after*."

Risk management surveys, risk assessments, and other proven methods for recognizing and then minimizing catastrophes should already be a given in your organization.

Should your situation end up in civil court, judges, attorneys, and juries will want to know if you did your best to head off problems before they began and what steps you took at the onset of any serious event to demonstrate that you knew whom to call (inside or outside your organization), when to call them, and what to have them do for you.

Chief Executive Officer

Director of Human Resources Development Person

The HRD officer may also have intimate knowledge of the labor relations issues facing the company, the existing quality of… it will be up to this person to manage and protect the human assets of the company as well as possible.

Director of Personnel

Director of Training

Hazardous-materials classes; first aid, CPR, and fire training; quality control, inspection, and production training; personnel, supervision, and management training; and any other programs that may be called upon in a court of law of the court of public opinion to demonstrate that the company is current, legal, and up to date in its procedures.

* *

Data and information protection strategies.

Should be cognizant of fire laws, hazardous materials issues, and all the other related compliance regulations that come into play whenever people and building come together.

By contracting in this fashion for legal services, they not only save money, but keep an attorney involved in the company's business on a peripheral basis. This avoids the need to locate or reintroduce a new attorney in the event that legal services become suddenly necessary.

The insurance specialists may have some suggestions as to ways to limit your risk, liability, and exposure to certain events or hazards based on their experience with their other clients.

Should a crisis situation arise, they will already by familiar with the firm's core message, values, and policies. This ongoing relationship can help them create the most favorable response.

(p.114)

CRISIS RESPONSE: A FIVE-STEP APPROACH

Step One: Initiate a Risk Assessment Survey

Step Two: Assign Roles and Discuss Duties

- *Authority:* Who has it?
- *Purpose*. What are the organization's main goals? What are the goals of the crisis response team, before, during and after a corporate problem that calls them into consideration?
- *Types of crisis events.* What types of crisis event, natural or man-made disasters, or other physical or psychological emergencies may affect the firm? In what areas is the company most vulnerable? Products? Services? Employees? Materials? Inventory? Image? Customer relationships? Transportation methods?

How will the company's people, places and things be most affected by any accident, crime, civil suit, natural, or man-made disaster? What do the members of the team fear the most? What events do they feel put the organization at the most risk of harm?

…How problems will be solved, what resources will be called upon, and who will take what roles.

(under step 4)

- Define specific types of potential crises as they relate to the business.
- Create optional steps to follow for each type of crisis.
- Describe the critical steps necessary to keep the business running during the crisis.
- Determine who would play what role to manage the crisis and keep the business running.

There must be an after-action review of both the incident and the steps taken to solve it. This postmortem period is critical if you want to avoid making the same mistakes again should the problem, or a derivative, flare up later.

APTRA

1. Anticipate
2. Plan
3. Train and practice
4. Review
5. Act (react, adjust, and move forward)

Anticipate

Decisions you can make today about something that might happen tomorrow, next week, next year, or, with luck, never, are a lot stronger than decisions you're forced to make in the heat of the moment.

"Things that are good for *one* portion of the organization are often good for the *rest* of it as well. New security measures don't just benefit the Security Department, they help everyone.

You start by gathering your sharpest minds. In large-to-midsize companies, this will probably come from your senior vice presidents, related personnel and HRD department heads, the security director, legal counsel, EAP representatives, and labor union stewards and other representatives. In smaller firms, the senior executive staff should meet and be prepared to discuss their functions and role.

Train and Practice

Consider creating the following mock scenarios:

- A power failure that lasts for more than one day
- A large industrial accident that has injured some of your workers and killed others.
- The public release of a video tape showing two of your employees engaging in criminal or inappropriate behavior (i.e. fixing phones, substituting old parts, driving erratically, smoking marijuana on the job, dumping waste products, sabotaging company materials, machinery, or products.
- A workplace shooting incident involving a former employee.
- A hazardous chemical spill that leaks fumes inside your facility and then later, out into the air.
- A suicide on company property.
- A phone call announcing the crash of one of your company cars, trucks, freight cars, or planes.
- A phone call announcing a customer's serious injury after using one of your products.
- A media report questioning the safety of one of your products.
- The on-site actions of agitators, protesters from outside your company, or labor union activists within your facility who create problems and get news attention.
- A media report from a disgruntled employee who claims that racial problems, sexual harassment, drug use, theft, or workplace violence is taking place inside your organization.
- The death, kidnapping or incapacitating injury of your CEO or other key executive.

Start by setting up a "war room" so that your crisis response team can meet as a group first.

Review

An ongoing review of your policies and procedures manual to clarify the rules of your organization and make sure you are staying within legal guidelines.

Good companies always review their actions and activities in the aftermath of any serious of significant corporate problem. They ask themselves:

- What did we do right?
- What did we do wrong?
- What were our strong points and what were our weak points?
- What surprised us?
- What were we completely prepared for?
- How well did we work, both as individuals, and as a group?
- What was our biggest area of liability?
- How well did we use our management and supervision roles and duties?
- Were there any telephone calls or announcements we forgot to make or should have made?
- How well did we handle the media?
- How well did we communicate our core message to the various interested publics inside and outside the organization?

- Did we protect our employees as well as possible?
- Did we protect the integrity of the company? Our records, hard assets, financial and personnel data?
- How should we adjust our contingency plans for an even better response in the future?

(p.126)
Stay with the works, change what doesn't, and always be ready to think outside the usual boundaries to solve the problem at hand.

Your firm's plan should not place or supercede your existing policies and procedures manual; it should supplement it. The standard policies and procedures manual is what guides your company the crisis management portion of it serves as adjunct planning an implementation documents to help company leaders think outside the normal envelope and deal with issues that may happen rarely or with such force as to cause serious damage to the organization.

Misuse of proprietary software that results in significant dollar losses, serious customer problems, or other injurious acts (financial crimes, embezzlement, virus plantings) calls for a crisis response.

Think of the written crisis response plans as if they were a fire alarm.

- *Keep it simple.*
- *Create a storage area for the crisis plans in each director's office.*
- *Use the crisis-planning opportunity to improve your current P&P manual.*

Media Rules to Live or Die by

- Don't lie
- Don't panic
- Don't lose control
- Don't get defensive

(p.171)

> Should you find yourself in a crisis situation, and you call the attorney for advice, you don't have to waste time and money acquainting him or her with you or the nature of your business, It becomes easier for the attorney to step into an assistance mode if he or she knows more about who you are and what you do.

There are two ways to protect you business during potentially serious situations: (1) have enough and the right kind of insurance; and (2) do the right thing.

The world of insurance-- assumed risk, injury or damage claims, liability issues, and hard dollars-- falls into your lawyer's domain as often as it does your insurance agent's, if not more so. Good attorneys will have copies of your insurance policies on hand and will at least be familiar with the language and coverage for each.

Your initial or ongoing liability reviews with your attorney should focus on what you both see as your biggest areas of concern in terms of risk. It may be the products you make, the presence of potentially hazardous substances you create of use to make those products, the types of work your employees do, transportation issues, or, in this ear of the database between employment at will versus the right to work, employee problems.

The frightening part is that if you're in charge and you allow certain conditions to flourish-- sexual harassment, workplace violence or alcohol abuse that causes stress claims or injury, or dangerous working conditions not covered by safety devices, training, or instructions-- you can become an automatic party to any litigation, even if you were not directly involved.

(p.180)

Emotions (i.e. "Screw those people! Let's fight it out!") should not be your guiding force. Your involvement in a court case should start and remain as a good "dollars-and-sense" decision, not one based on who is bigger or smarter. Wisdom based on experience, intelligent suggestions from your legal counsel, and plain common sense should be your ongoing guide.

When *should* you consider settling, and when should you fight it out in court? Today we have insurance policies and claims adjusters who are paid to make that decision for you.

The above summary has been provided to you compliments of Altfeld, Inc.