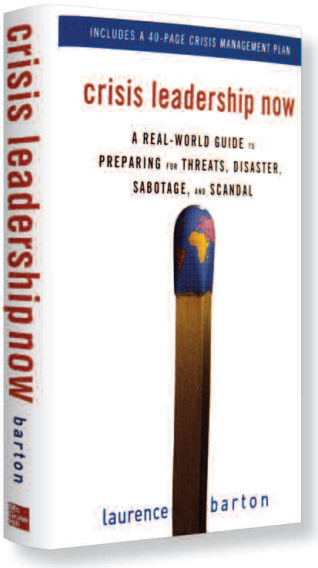
May 2008

SOUNDVIEW Executive Book Summaries®
www.summary.com

Leadership: Strategies

Crisis Leadership Now

A Real-World Guide to Preparing for Threats, Disaster, Sabotage and Scandal



by Laurence Barton

THE SUMMARY IN BRIEF

Some managers shine during a high-level crisis, while others stumble. Leading crisis management expert Laurence Barton explains why those with an action plan in place are the ones who can react quickly, manage rumors, and respond to victims and stakeholders sincerely and adequately while keeping their organization afloat. As a crisis leader, you must follow a comprehensive protocol that includes the implementation of teams, systems and tools to respond to a crisis and recover from its impact.

In his seminars with executives, Barton begins by asking, "What's the worst that could happen?" The results are surprising. On top of the expected, such as workplace violence, product recall, violent weather, pandemics, chemical spills and terrorism, executives have reported actual crises such as food poisoning impacting hundreds of guests, a counterfeit product uncovered, devaluation causing massive financial loss, and extended loss of electricity.

Barton first addresses how to avert crises through measures such as a program for securing your workplace, proper management of workplace threats and adoption of rigorous human resources practices. Next, he covers disasters including terrorism, industrial accidents, stormy weather, pandemics and sabotage. He then gives specific plans for communicating during "Code Red" situations.

IN THIS SUMMARY, YOU WILL LEARN:

- How to assess your crisis risk.
- Ten actions you should take now to decrease your vulnerability to risk.
- What to do in the first eight hours of a major crisis.
- What the OSHA requirements are for instituting an employee awareness program about the four basic types of workplace crimes.
- How to develop a stakeholder's analysis during a crisis.

CONTENTS

Published by Soundview Executive Book Summaries, P.O. Box 1053, Concordville, PA 19331 USA

Concentrated Knowledge™ for the Busy Executive • www.summary.com
Vol. 30, No. 5 (3 parts), Part 1, May 2008 • Order # 30-11

THE COMPLETE SUMMARY: **CRISIS LEADERSHIP NOW**

by Laurence Barton

The author: Dr. Laurence Barton, former vice president of crisis management at Motorola, has spent 25 years studying the causes of crisis in the workplace. He has managed more than 1,200 incidents worldwide, writing crisis plans and consulting with senior management at ABC News, The Walt Disney Co., Nike, Honda, British Petroleum, ESPN, and more than 60 hotels and casinos during defining moments.

Crisis Leadership Now by Laurence Barton. Copyright © 2008 by Laurence Barton. Summarized with permission of the publisher, McGraw-Hill. 346 pages. $39.95. ISBN 0-07-149882-1.

For additional information on the author, go to http://my.summary.com

Secure Thy Workplace!

You can often judge how much a company values corporate security by looking at where it places the physical offices of its security managers. Sometimes you'll find them in the basement, right next to the soft drink machine. In these companies, the primary function of the security director is to ensure that the CEO gets to and from the airport in the company Escalade on time.

There are exceptions: Companies such as Disney, Emerson and Coca-Cola give credence to their security leaders and listen to them about crisis planning. They get it: The best crisis is the one that has been prevented. A smart security director understands that his or her company must be counterintuitive.

10 Questions to Benchmark Your Security Team

Here are 10 questions that are commonly asked when your firm is being audited, from a security point of view:

1. What's the average number of hours that your security guards are trained by you or your company?

2. What's your annual turnover in security personnel?

3. How many of the leaders in your security organization have a bachelor's degree from an accredited college? What about a master's degree?

4. Has your director of security ever worked at another company in your industry?

5. Has your company ever conducted an audit of your top talent to determine if they leave confidential memos and reports out that others can read or copy after hours?

6. What is the relationship between your director of security and your leadership in IT? Do they even know each other?

7. How many times in the last year has the security director spent a day at each major site in the company — at either your various sales offices or key facilities?

8. Has the security director ever invited the regional office of the FBI, the Postal Service or others to provide an annual briefing on potential corporate threats?

9. Does human resources routinely call upon security when a problem employee is about to be exited?

10. How many of the books on the security director's shelf have been published in the past five years?

Preventing Crisis: Background Checks

One way to prevent crises is to perform background checks regularly. Insist that a qualified employment verification firm complete the following checks on any potential employees:

- Validate that the candidate is using his or her true name.
- Check for a history of credit fraud.
- Verify that the Social Security number the candidate provided is that of a living person (a surprising number of applicants will use the number of a deceased relative with a similar or same name to hide a checkered financial past).

If one or more of the previous checks turns up questionable information, continue researching the candidate:

- Does the person have a genuine physical address or is the person using a mail receiving/forwarding service?
- Is the person living in a hotel/motel/temporary residence?
- Does the person frequently use a check-cashing service or does he or she have a legitimate checking account?
- Does the background check show any time lapses in employment? While the person could have been caring for an aging parent, it could also correlate to time spent in a correctional institution.

Keep a specific eye on applicants' criminal records for financial or "white collar" crimes. For the most part,

1-800-SUMMARY
service@summary.com

Published by Soundview Executive Book Summaries (ISSN 0747-2196), P.O. Box 1053, Concordville, PA 19331 USA, a division of Concentrated Knowledge Corp. Published monthly. Subscriptions: $209 per year in the United States, Canada and Mexico, and $295 to all other countries. Periodicals postage paid at Concordville, Pa., and additional offices.

Postmaster: Send address changes to Soundview, P.O. Box 1053, Concordville, PA 19331.
Available formats: Summaries are available in print, audio and electronic formats. To subscribe, call us at 1-800-SUMMARY (610-558-9495 outside the United States and Canada), or order on the Internet at www.summary.com. Multiple-subscription discounts and corporate site licenses are also available.

Rebecca S. Clement, Publisher; **Sarah T. Dayton**, Editor In Chief; **Melissa Ward**, Managing Editor; **Christine Wright**, Senior Graphic Designer; **Nan Bauroth**, Contributing Editor

Workplace Violence Policy

U.S. employers are required by the Occupational and Safety and Health Administration (OSHA) to have both a policy and a training program that inform employees of the proper methods of sharing and reporting concerns about intimidating and threatening workplace behavior.

criminal background checks are retained by research firms for only seven years or less. Many of the more accomplished research firms will look for incidents such as arson, weapons violation, simple assault, domestic violence, substance abuse, etc.

Managing Threats and Workplace Violence

In the vast majority of workplace violence cases, the perpetrator is acting on a real or perceived grievance. The person may have been denied a workers' compensation claim and is now experiencing physical pain while at work, or he or she may have been reprimanded in front of peers and is now embarrassed. Maybe the employee was dismissed or reassigned, causing the person to seek revenge on a supervisor in an effort to regain control of life. No matter what the employee's motivation, the real question is: Are we *listening*?

Consider the range of potential threats:

- Stalking of an employee by a former spouse, partner or co-worker.
- Threats to bring a weapon to work, possibly preceded by a sarcastic comment; or "accidentally" leaving a hunting rifle in the back of an auto for others to see.
- Comments made by a former employee that are intentionally provocative in nature.
- E-mails or posted blog messages that threaten the life of a co-worker.
- Behavior intended to cause concern, such as mimicking the gesture of firing a weapon at a co-worker.

Assessing a Threat

Many industries, such as retail, health care and hospitality, are dependent on a high degree of interaction with clients who are total strangers. Companies in these sectors sometimes offer security supervisors and customer service managers a basic primer in managing hostile persons. Although there is no single model, we have learned much in recent years regarding specific behavioral and clinical signs of those who pose a *potential risk* to themselves and others.

Many companies have a threat assessment team whose members represent their human resources, security, IT, EAP and legal departments. The team is typically deployed when an employee makes or poses a threat. In many cases, the team will be supplemented by the supervisor of the problem employee. These teams sometimes turn to external threat assessors to gauge whether an employee outburst could escalate into violence and, most important, whether the person has the *capacity* to act on his or her threats.

It's not enough to say you will consult with a psychologist when a challenging situation arises. You need to remember that employers can be charged with tort liability for failing to prevent someone from hurting him- or herself or someone else. Managers should remember that virtually every employer has three paramount duties when threats arise:

1. Duty to Care: Saying you care isn't enough. What if someone causes harm and media later report you were *previously aware* this person made threats? What did you know and when did you know it? What did you do about it?

2. Duty to Warn: Sometimes a perpetrator acts without warning. But there are often *pre-incident indicators* before an assault at work. From the moment you are aware of such threats, assume you have a Duty to Warn others. One way to minimize exposure is to confer with legal counsel, security and HR. But think about how to warn others. Risk communication involves a collaborative discussion about the advantages or drawbacks of a small group meeting, a memo, an individual session with potentially impacted people or other options. Involving law enforcement in these is encouraged.

3. Duty to Act: You may have an obligation to act when an employee informs you that he or she is being harassed or threatened. Common steps include offering the employee a cell phone to call police coming to or from work if threatened, hiring an external security firm to patrol the parking lot until a restraining order is achieved and documenting all suggestions you make to the employee to work from an alternate location, if possible.

Now It's Your Problem

The public expects you to understand the basics of threat assessment when your company is faced with possible workplace violence. Basic facts to consider:

- A violent past is the single best predictor of future violence — period.
- An employee's interest in and access to weapons are certainly critical factors.
- Even physical appearance should be considered, e.g., people contemplating suicide often provide physical warning signs to others in the days preceding the act.

For information on how to assess an individual's "Fitness for Duty," go to http://my.summary.com

OSHA expects employers to offer awareness programs regarding the four primary types of workplace crimes:

1. Crimes committed by an individual with *no connection* to the workplace, such as a homicide during a robbery.

2. Aggression *targeting employees* perpetrated by customers, clients, patients, students, inmates or others for whom you provide a service or product.

3. *Worker-against-worker* violence, such as between a manager and a subordinate, or a former employee who returns with intent to injure a former supervisor.

4. Aggression stemming from a *personal relationship,* such as a former business partner who returns to the work site seeking revenge for a financial disagreement.

Understanding Threats

Once a manager is aware that a problem employee is exhibiting disturbing behavior, a threat assessment team should review several key issues in a timely manner. Begin by evaluating specific content of the threat. Does it explicitly suggest intent to do harm? Then review the capacity, skill set and mental state of the person posing the threat. Who is this person? Where is the person now? *How* is he or she?

Even when a person has no intention to do harm and merely verbally expresses a threat, others could still be psychologically harmed by enormous fear. When an employee tells you he or she feels that a co-worker may do him or her harm, you should take the employees' comments seriously and act on the warning. Document what the person said and the response actions you are taking. Involve law enforcement when appropriate. ●

Negligent Hiring and the Role of Human Resources

Thirty years ago, few employers admitted publicly that they had problem colleagues in their ranks, and society was more focused on corporate environmental abuse than on employee malfeasance.

Even though people haven't fundamentally changed over the decades, technological advances, such as the Internet and camera phones provide a better periscope through which to observe bad behavior, both on and off the job. We also know that numerous scandals in recent years surfaced because information that employers thought was confidential became public.

To immunize against a future problem, you should do five things:

1. Interview each new candidate for an executive position at least twice, and at least two people should interview each person in detail so you can compare notes.

2. Conduct a thorough criminal, financial and sexual predator background check on each new hire.

3. Ask a key interview question: "Tell me about a highly stressful situation involving a former co-worker and how you resolved it."

4. Once you suspect someone on your payroll is a potential problem, promptly investigate allegations.

5. If you sit on a board and signals emerge that a current leader has possibly engaged in malfeasance or behavior contrary to core principles and stated values, hire an independent investigator to discreetly examine the allegations.

Effectively Managing the Downsizing Conversation

Psychologists have written that the death of a child or spouse, the loss of a job and a separation from a spouse are among the worst possible moments of a person's life. If you have been selected to have the "downsizing conversation," you are about to share one of those three moments with one of your employees — that he or she is being laid off. With care, rehearsal and confidence, you can navigate this difficult task well.

The goal is to meet with the employee, deliver the news of the layoff, walk the employee through the severance package that he or she is receiving and communicate clearly what needs to be done immediately (collection of building keys and employee ID cards, cleaning out the office, etc.). Separation discussions should last no longer than seven minutes. ●

For additional information on how to manage the downsizing conversation, go to http://my.summary.com

Managing Health Crises

Most of us live in denial when we consider our vulnerability to possible pandemics: We are aware that flu outbreaks wiped out millions of people a century ago, but we expect modern medicine to rush to our aid in the event of another public health calamity.

A crisis team will greatly benefit your organization, both before and during any major transnational health crisis. That team ideally will be composed of those who can help you anticipate the impact of declining health on your people and operations. A number of Fortune 1000 companies already have developed pandemic plans — this doesn't mean they're fatalists. Rather, it means they understand their fiduciary responsibility to protect their employees in every jurisdiction, their duty to think about how they could deploy aid to expatriates and their families living abroad, and that they likely will be notified of an outbreak only after a significant number of people have become symptomatic.

Now It's Your Pandemic

Most companies have never asked: What if 30 percent of our workers become sick and are incapable of working? What if customers stop buying our product because they are hunkered down at home? If a pandemic were to force curtailments in global trade, even for 30 days, products wouldn't be shipped, services couldn't be sold, and income would come to a halt.

Here is a checklist of issues to consider when drafting your pandemic plan:

- Identify who will "own" the logistics of communicating breaking news about the health issue to the general population so there is a single channel of communication.
- Determine who is currently traveling, where they are today and whether/how they can get home.
- Identify one leader who will communicate your plan to your employees, and encourage that person to work from home. Then determine how IT will support telecommuting and how customer support needs will be managed. Will your company servers be able to withstand the crisis?
- If any business traveler has just returned from an impacted region, he or she may need to see a doctor. There will be legal issues about what you can and cannot order an employee to do.
- If products are shipped to or from overseas, a logistics emergency plan is needed, detailing how you will receive/send future shipments given a potential embargo.
- Assign a content manager for your company intranet and public Web site to communicate key details about preparedness, slowdown or shutdown in a timely manner.
- Consider the impact that prolonged salary and benefit continuation will have. If you work with a union, engage leaders early on so that parties are able to reach accord on major decisions.
- Arrange for regular conference calls to various company departments so employees, contractors and vendors can update one another on key developments, projects and when they anticipate returning to work.
- Identify succession planning for mission-critical people.
- Update home, cell and emergency numbers for each employee, key supplier and contractor, and ensure that multiple leaders have access to this confidential database.

Industrial and Environmental Disasters

Inevitably, management teams avoid contemplating accidents of an industrial nature. This is for two principal reasons.

First, the scope of the damage that can arise from industrial accidents is incredibly wide. Many crisis managers find it difficult to prepare their management framework for the dozens of potential scenarios that could impact their organizations.

Second, unlike cases of workplace violence or natural disasters, many managers tend to believe that their lawyers will be able to apply the same crisis standards that generally seem to work when other types of incidents arise. As a result, managers often suggest that their lawyers spend less time on these issues because of the (false) assumption that legal counsel understands the nuances of such complicated matters as technological science and construction dynamics, which are unique to industrial accidents.

Factors to Consider in Industrial and Environmental Disasters

As you begin the process of assessing your company's vulnerability to industrial accidents, you'll want to consider a variety of factors, including:

- Proximity of facilities to underground and above-ground oil, natural gas and other utility lines.
- Proximity to major highways and rail lines where toxic materials are transported.
- Chemicals kept on-site, who manages them, and a history of industrial incidents or recent regulation infractions.
- How many projects may be going on at any one time that require external contractors, and what competencies and equipment they need.
- Preparedness level of local first responders to major issues such as contamination or release of a toxic cloud nearby, and their ability to orchestrate evacuations and issue widespread alerts.
- Last time senior management focused on waste management, local pollution controls and impact on wildlife in the event of a toxic chemical spill on-site.
- Who is monitoring the driving records/licenses of those operating company vehicles, delivery trucks and special equipment.
- Adequacy of on-site medical response and safety systems to address first tiers of an industrial accident.
- Who monitors/investigates incidents or near-misses at your facilities.

Sabotage: The Undisclosed Crime

Today's saboteurs take many forms and are not always easily identifiable, but they can cause genuine security risks when they infiltrate air defense or public safety systems. Your enemies may include former or current employees and contractors, competitors or investors eager to manipulate chat rooms and blogs to profit from a significant move in your stock price.

Unlike robbery, which is typically reported to local law enforcement, sabotage is a different kind of crisis for a business. Supervisors are often hesitant to report incidents because they fear local press will report them, causing the company embarrassment and potentially further economic loss. In some cases, leaders of a company may not even know their databases or equipment have been sabotaged. On suspecting sabotage, many companies will hire investigators, who sometimes engage in social engineering to try to track down and prosecute the perpetrator. There is no science to combating such threats; sabotage is a complicated crime and its impact on business is often significant — and sometimes deadly.

The Inside Job

Sabotage is not the result of a spontaneous act of revenge; it requires planning, knowledge, access and usually some self-exposure on the part of the saboteur. A catalyst or motive is always present, even if the acts are driven merely by self-gratification. An individual with access to your systems and controls has a far greater chance of penetrating the safety of your core operations.

Chances are your business has property and casualty insurance, director and officer insurance, errors and omissions coverage — but do you have cyberinsurance? Your failure to protect sensitive data about employees, customers and others could be a violation of the Gramm-Leach-Bliley Act.

The Four Principal Categories of Sabotage

The following are four principal categories of sabotage that can have an impact on the business and government sectors:

1. Human resources-related. "Getting even" is a priority for some people and the methods they employ can be costly and often difficult, if not impossible, to track.

2. IT and mechanical. The impact from one act can cost you millions in lost production due to equipment malfunctions and time delays.

3. Economic. Unethical competitive intelligence-gathering is an arena with former Russian spies, current Korean government ministers and many others who find a way to get themselves on the payroll of a company they're seeking to destroy.

4. Reputational. Bankruptcy is not sabotage, but when a company is on the brink of failure, competitors, eager to build market share, may spread rumors, increase attempts to poach top talent or engage in other acts that can be considered sabotage.

Applying Strategic Standards

Here is a recommended five-stage approach to preventing sabotage:

1. Assess your risks and look at internal controls, including HR practices.
2. Design policies and procedures that recognize it's a new world.
3. Embed an antifraud program into your culture now.
4. Engage all stakeholders in discussions about retribution and sabotage.
5. Create a robust investigative process.

Communicating When It's Code Red

Executives are largely uncomfortable with crisis communications. In a typical day, your senior management is working in a known world where customers, products, the supply chain — all of which constitute the principal ingredients of business — are predictable. There's no way to know when a crisis will hit. Events are disruptive, and damage can last for weeks, even months, and most likely will be costly. As a result, management is often overwhelmed by the velocity and disruptiveness of corporate crises.

Diagnostics: Asking Questions Before Communicating

Here is an outline of a due diligence and crisis communications plan presented to an emergency meeting of a bank board because the bank's president was involved in some potentially embarrassing activities outside the office. The three principal questions that would define the crisis communications plan were:

1. What do we know?
2. When did we know it?
3. What are we going to do about it?

Questions pursued with the bank's legal counsel, VP of HR and several board members included:

- Did the person engage in inappropriate or *illegal* activities? Were her actions a violation of a specific standard in the company code of conduct? The difference between inappropriate and illegal is profound in terms of how the bank might communicate any decisions about her future.
- Is the bank president known beyond the bank's high-net-worth clients, such as being a high-profile member of any community/charitable groups?
- Since the bank is publicly traded, the SEC, FDIC and state banking commissioner might have questions about due diligence and whether the president broke any laws. Did the bank hire a private investigator to verify the allegations, and if so, what was found? Is the report discoverable if her behavior leads to legal action?
- Did any bank employee engage in whistle-blowing that led to the allegations? If so, what protections will the bank provide that person? Could there be additional facts that

will be disclosed in days to come that could make this situation worse, further impairing the bank's reputation?

• Are there any major events (e.g., a quarterly earnings report or new branch opening) in the next few weeks that should be reconsidered if the allegations become public?

• If the president is terminated, can she sue the bank, and if so, on what grounds? What is the bank's succession plan for leadership personnel?

In any crisis, a smart communicator will ask these and other questions to help frame his or her crisis communications plan. Twenty years ago, a news release indicating that an executive was departing "to pursue new interests" was commonly used. Although there may have been a few inquiries, the majority of management time was spent managing rumors, not preventing speculation. Today, in a world where the spirit of disclosure places a high value on ethical management and organizational culture, companies must anticipate provocative, legitimate questions.

The Eight-Hour Window

When a crisis is confirmed, the wheels of response should begin turning. This is a chaotic and unsettling time, no matter whether the organization is facing the impact of an earthquake or a violent employee. Regardless of the scope of the incident, the communication demands can be overwhelming and must be managed well.

Companies such as Procter & Gamble, British Petroleum, Kraft Foods and others recently have begun to standardize the process of harnessing key organizational resources and bringing definition to their crisis communication plans *within the first eight hours after an incident arises.* Decades ago, companies looked at crisis communications in terms of the "news cycle," believing that updates only would be shared with reporters before the three principal television newscasts of the day at noon, 6 p.m. and 11 p.m.

Our Web-centric world has effectively ended the news cycle. We have gone from three news cycles a day to dozens. The eight-hour window is a general standard, not an Olympic-timed event. Yet this time frame is a credible goal that many crisis communicators seek to achieve. If you can capture what has happened, who is impacted and how you intend to communicate your response with a clear plan of action within eight hours, you have a foundation for an excellent recovery plan.

To stay ahead of the headlines, there is a road map to effective crisis communications that should be followed. First, create a fact sheet on the scope of the incident, including names of victims and family, as well as witnesses and a time line of how events unfolded. Update it every hour as needed.

Verify all facts with law enforcement and company security and determine who should contact victims and family members, as well as whether your claims or legal department should be involved in personal visits to affected families.

Following the fact verification, begin to draft a response to the big three questions (What did we know, etc.). Continue refining based on new information.

Next, prepare a brief statement for phone operators so they know what they can and cannot say. Emphasize that they should refrain from speculating or saying anything beyond the script. All media inquiries should be directed to appropriate spokespeople. Voice mail of all senior leaders and spokespeople should be checked continually, as new facts may emerge. Rumors may spread. Regulators or elected officials may call. In most companies, communicate known facts with employees first (such as a plane crash claiming the life of an executive), but in other cases consumers may be the first ones to notify (such as a toxic chemical leak near or at a facility).

Finally, each stakeholder category may have unique crisis communications needs, for example employees may want to know if they will be paid even though they are told to stay at home during a chemical cleanup. Customers need to know when products will arrive. News media will have other questions. Your communications team should designate one person per stakeholder category to "own" the communications process with that category.

The Basic Crisis Communications Inventory

A crisis communications plan benefits every organization from nonprofits to multinational hedge funds. To achieve a high level of preparedness, your organization should have a basic communications inventory.

1. Outline the hierarchy of who will speak for the company, and include office, home and cell phone numbers of the crisis team, crisis counselors, legal counsel and insurance company.

2. Designate where you will meet, who owns the telephony aspect of your response and who will activate your crisis alert system.

3. Embed in your plan a simple outline of core crisis messages that you can customize. You'll never know all the facts immediately. So qualify all remarks with statements like "Based on what we know at this point ... " If you make a definitive statement and later have to reverse your message, your credibility is compromised.

4. Identify the 20 worst questions you could be asked during any Q-and-A session with the media or public. If possible, conduct a mock news conference first. Keep your opening statement to two minutes or less. Let the press ask questions. You will be allowed reasonable time to reflect on your answers.

5. Publicize your actions through media networks

such as PR Newswire, which has teams that know how to reach reporters and editors quickly.

6. Frame the crisis properly. Is it an incident? A crisis? Do you have all the facts? If not, say so. Admit what you know and don't know. Stakeholders will have sympathy if you acknowledge that your colleagues are feverishly working to gather all the facts. Tell them you have deployed teams to the site and promise to return with more information in a timely manner.

7. Ask media to help. Airline spokespeople after a crash inevitably begin with statements about thoughts and prayers, then explain the itinerary, type of aircraft, etc. They avoid confirming names of victims or survivors until law enforcement officials have notified next of kin. Typically, a company representative will accompany police when they visit victims' families. Airlines also share an 800-number so loved ones can call and ask for more information. ●

Crisis Prevention and Response: Picking a Consultant

Most executives have no idea what crisis preparedness tools their business needs until a crisis strikes. That is why they often contract outside consultants. Among the services that a consultant can provide are:

- Evaluation of your existing preparedness plans
- Assessment of worst-case scenarios based on your industry and market position, who should respond and how customer support would continue
- Refinement of notification and decision-making processes as well as resource allocation; this is especially useful during weekend and after-hours incidents
- Preparation of a comprehensive list of response tools, including medical and telecommunications needs, that your enterprise may not currently have access to.

Finding a Crisis Consultant

Be wary of consultants who are eager to offer you much more than an overview of their credentials and capabilities. When you interview a consultant about the crisis assessment he or she may perform for your enterprise, ask how detailed and customized the final document will be; whom he or she intends to interview in the preparation of the proposal; the types of questions that will be asked; and how many risk or crisis management plans he or she has created in the past. ●

Assessing Your Crisis Risk

Begin your evaluation of your organization's exposure to a potential crisis by completing this assessment of key categories of risk. This is often best accomplished by asking a team of your associates to work with you in a planning meeting. Rank the following items on a scale from 1 to 10, with 10 representing the greatest damage and 1 being the least.

1. Threats against individuals.
2. Major fire or flood at key facilities.
3. Power failure and sustained loss of utilities.
4. Pandemic flu sweeps across region of your enterprise (expected temporary loss of 30 percent or more of your work force for more than three months).
5. Bomb or bomb threat at your facility.
6. Terrorism specifically aimed at your company, people and facilities.
7. Terrorism (not aimed at your company) in a region that disrupts business travel, product shipment or port functions.
8. Exposure to a product recall.
9. Alleged compliance violation (e.g., European Union Act Tariffs or allegation that a salesperson violated the Foreign Corrupt Practices Act).
10. Geopolitical instability in core markets disrupts supply chain.
11. Sole source provider is destroyed or impaired.
12. Major currency issue causes significant devaluation (20 percent or more).
13. Community protests by residents or union activists.
14. Organized boycott of company.
15. Competitive intelligence threat; theft of customer/financial/data design.
16. Widespread counterfeit product and/or adulteration.

Don't run and hide from crisis preparedness. There's hope. Your organization has you, and you can also groom and hire talent that has experience in risk and crisis management. There are tons of government resources available if you know how to source them, and the public's general awareness of crisis leadership has never been higher. You're in a sweet spot. ●

RECOMMENDED READING LIST

If you liked *Crisis Leadership Now*, you'll also like:

1. ***Judgment* by Noel M. Tichy and Warren G. Bennis.** Whether you're discussing former United States presidents, Fortune 500 CEOs, military generals or college hockey coaches, leaders are remembered for their best and worst judgment calls.
2. ***The Wizard and the Warrior* by Lee G. Bolman and Terrence E. Deal.** Bestselling authors Lee Bolman and Terrence Deal give leaders the insight and courage they need to take risks on behalf of the values they cherish and the people they guide.
3. ***Confidence* by Rosabeth Moss Kanter.** Presidents, managers, coaches and even individuals have the power to choose how they deal with a loss and whether they are going to allow it to be the beginning of a trend or whether they have the confidence to learn how to win next time.