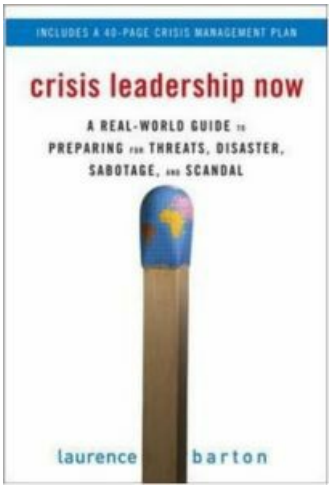

Book Crisis Leadership Now

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

Laurence Barton
McGraw-Hill, 2007

Recommendation

Managing an organization is an awesome challenge during the best of times, but far harder in the worst of times. Every process and problem becomes infinitely more difficult when a disaster strikes, be it an act of terrorism, an industrial emergency, fire, flood, earthquake, hurricane, corporate crime, scandal, epidemic, mass murder – you name it. Alas, the old saw that anything that can go wrong will go wrong is often true. Is your organization prepared? Studying this book by crisis expert Laurence Barton is a good way to get ready. He details practical, time-tested responses to disasters of all types. Most crises arrive without warning, so solid preparation is vital, and denial will get you nowhere fast. If you are a CEO, a communications professional or a senior executive, *BooksInShort* advocates reading this very practical book – before the deluge.

Take-Aways

- Many organizations are poorly prepared to handle emergencies.
- The number of different emergency events and scenarios that can hamstring an organization is staggering.
- Organizations often operate in a state of blissful denial that a disaster will ever occur.
- When it does, few organizations communicate effectively.
- Be prepared to communicate details about the event, to provide a timeline, and to outline your company's actions to address or mitigate the negative effects.
- A crisis requires one commander for tactical control and one spokesperson for message control.
- In any crisis, before anything else, take care of the victims. Plan to have an "emergency operations center."
- To prepare for a disaster in advance, designate a supervisor, management teams and an off-site facility for IT backup.
- Set up another team to focus on business continuity after the event.
- The best way to deal with a crisis is to prevent it in the first place. This is not always possible.

Summary

Are You Ready for a Crisis?

Few organizations are prepared for crises or ready to handle disasters. Indeed, many are incompetent at crisis planning, management and communications. Here are some prime examples:

- Corporate thieves stole millions of customer credit card records from TJX, the corporate parent of Marshall's and T.J. Maxx retailers, due to its inadequate security system. When the media asked about the theft, TJX reps hid behind "confidentiality." The company also failed to notify customers promptly.
- In 2004, an employee at Friendly's Ice Cream Restaurant in Arlington, Mass., came down with hepatitis. As a result, thousands of diners immediately needed immunoglobulin injections. The media jumped on it. Alas, Friendly's treated the event too casually, so people stopped eating at the suddenly "unfriendly" outlet, which soon closed.
- During a *Dateline* taping for NBC, reporter Brian Ross showed Wal-Mart CEO David Glass an NBC video reporting that small Indian and Pakistani children were working in brutal sweatshops run by Wal-Mart subcontractors. The kids were sewing clothes later marketed as "Made in America." Ross asked Glass to comment: "Terrible things happen in this world," he said lamely. A Wal-Mart vice president walked in and abruptly ended the interview. NBC aired Glass' dumb

remark and Wal-Mart's ham-handed shutdown.

"Crisis management is uniquely focused on how to respond to victims, employees and other stakeholders during those precious first eight hours of your situation."

What accounts for such slapdash planning? Many companies appear blissfully unaware that a crisis could hit. Yet the potential disasters are unlimited: threats of violence, floods, war, hurricanes, fires, tornadoes, power failures, pandemics and terrorism. Businesses also can face manufacturing or product problems, like recalls, counterfeiting, boycotts, "compliance violations," supply chain disruptions, union problems, community protests, corporate thefts and scandals. It only takes one crisis to create chaos. Do you have contingency plans?

Violence in the Workplace

Employees can be the perpetrators or victims of violence at work. Unfortunately, many senior managers act as if violence cannot occur at their sites. They are mistaken. More than 8,000 violent episodes occur daily in U.S. workplaces. Stalking and domestic disputes are common. So are e-mail threats. To guard against hiring potentially violent employees, HR departments should thoroughly examine prospective workers, including checking for any past criminal activity.

"Even the most stellar business leaders in the world can stumble in a crisis."

To sniff out a potentially problematic employee, use this question in the middle of an interview: "Tell me (those are the pivotal, operative words) about a highly stressful situation involving a former co-worker and how you resolved it." A person who claims that no such incident ever occurred around him or her probably is lying. You are looking for a response that indicates, "no surprises, no anger, no drama." This will show what the candidate deems stressful, and how he or she handles conflict resolution. It also can offer some clues about his or her emotional make-up.

Health Crises, Violent Weather and Other Disasters

Pandemics or epidemics can close your company with surprising speed. Does your organization have a plan for infectious or hazardous emergencies and other medical issues? It should. Prepare also for vile weather. A tornado or hurricane can put you out of business. Consider Hurricane Katrina, the devastating, $150 billion storm that leveled New Orleans. Industrial disasters, terrorism or sabotage also can be devastating. Build your contingency plans accordingly.

"Communicating When It's Code Red"

When disaster strikes, your organization must communicate about the situation to its employees, customers and investors, as well as the media and the public. Before anyone starts talking, answer three vital questions: "What do we know? When did we know it? What are we going to do about it?" You have only about eight hours to tell your story. After that, you will have ceded control of the story to others, like the media. To manage crisis communication, track these primary points:

- Develop a formal crisis communications plan in advance of any crisis.
- Create a fact sheet that details the event's scope and its timeline. List victims and witnesses. Routinely update it. Confirm all facts.
- Establish who within the organization will contact victims.
- Develop responses to the predictable questions: why, what, when and how.
- Prepare statements or scripts your telephone operators can use with callers.
- If possible, communicate first to your employees, then to other constituencies.
- Respond to each relevant group, like investors, customers, staff, the media and the public.
- Designate a single, fully prepared spokesperson. Have him or her rehearse responses to the 20 worst imaginable questions.

"Crisis Response and Recovery"

Your organization's crisis plan should designate a senior-level "corporate crisis management team" to report to the CEO, evaluate the extent and future scope of the disaster, and operate as long as needed. Set up an overall incident commander to handle tactical issues and work with the CEO, an "organizational crisis management team" to focus on resuming business, a business continuity plan coordinator and a communications manager.

"An emergency is any incident, potential or actual, which seriously disrupts the overall operations of your enterprise."

When disaster strikes, take these immediate steps:

- **"Respond first to victims"** – First make sure the victims get help. Coordinate first responders. Inform senior management about the scope of the event. Activate the corporate crisis management team and have it gather facts. If need be, open a 24/7 "emergency operations center" (EOC). Implement the communication plan. Issue a brief on the status of the crisis every 30 minutes. Activate the organizational crisis team to consider how to restart operations.
- **"Respond second to organization"** – Maintain the EOC. Begin media communication using one spokesperson only. Brief your legal counsel and insurance carriers on any exposure ramifications. Conduct rehearsal press conferences for the CEO. Log all calls.
- **"Respond third to publics"** – Have the CEO or another senior executive lead a press briefing. Focus on the victims and the company's actions. Communicate fully to your employees and customers. Document all major decisions, along with dates and times.
- **"Respond to recovery needs"** – Keep the corporate crisis team updated. Survey employees, customers and other stakeholders to see if the response meets their needs. Coordinate with underwriters to be sure claims are met quickly. Make sure those affected get the help they need.

"Every day around the world, people engage in acts of retribution and sabotage."

Events should unfold in roughly this order, depending on the situation:

- **Post-crisis: "first eight hours"** – Deal with the most dangerous circumstances immediately. Activate the emergency operations center to take care of victims. Make sure first responders get everything they need, when they need it. Assess the extent of the disaster. Initiate communications. The organizational crisis team should meet at least twice daily. Finance should track all costs. Establish supplier and vendor contact as needed. Organize follow-up psychological counseling for those who need it.
- **Post-crisis: "eight hours and beyond"** – The incident commander works with the corporate crisis team to make all the vital decisions. The organizational crisis team should implement the incident commander's directions and respond to the needs of victims, employees and the community. Hire contractors as required for "smoke and water removal, debris removal," damage control and repairs. Implement an information security plan. Set up a "shadow Web site" to communicate with all groups. Establish a "company emergency hotline" for all employees. The business continuity plan coordinator should make sure your program is in effect.
- **Recovery** – Develop a plan with target dates for facility repair. Have your legal counsel review all due diligence requirements. Continue to assess the damage. Deal with all utility providers. Keep adequate cash on hand. Develop special compensation incentives as required. Stay on top of all logistical requirements.
- **"Message plan"** – Guarantee action. Stress organizational values. Assume full control of all press briefings and related activities. Immediately correct any misinformation.

  "We are in the midst of an unprecedented holy war aimed not only against governments but also against business."

Heed these basic "crisis management and recovery plan" considerations:

- **"Before the crisis"** – Designate corporate crisis and organizational crisis team members and operational managers to get things back to normal after a crisis. Plan an "IT recovery site." Meet semi-annually to discuss the crisis response plan. Update and share the communications plan often.
- **Primary players** – Designate an "incident commander" to manage the crisis tactically. Designate a leader from the communications department to manage the message. Legal counsel should coordinate with insurance brokers about your firm's fiduciary responsibility, if any.
- **"Measuring disruption"** – Your organization must assess the extent of the disaster.
- **"Finance and accounting"** – What is the financial damage? What is your liability? Insurance coverage? Anticipated losses? Impact on quarterly earnings?
- **Communications** – Immediately activate a communications response team. Depending on the emergency, their job may continue without a break for a long time. Make sure the emergency operations center is fully staffed and has back-up power and emergency supplies. Ensure open communications between headquarters and the crisis site. Be prepared in case your leaders need an alternate site with adequate IT and telecommunications. Communicate openly with the media and the public.
- **IT** – Is connectivity operable? What about data and equipment loss?
- **"Sales and marketing"** – When will production re-open? If apropos, do customers get refunds? Will you advertise during the crisis? How will you update major customers?
- **Security** – Coordinate completely with law enforcement. Did surveillance cameras videotape the event? Are any perpetrators employees? Customers? Other stakeholders? Have you restricted access to the site? Do you need more guards? Did you have warnings? Do you have a script for telephone personnel and receptionists?
- **Human resources** – Acknowledge all victims and heroes. Coordinate with legal counsel regarding restitution or compensation. Institute an employee communications plan.
- **Legal** – What obligations await? Heed your "duty to care, duty to warn and duty to act."
- **Strategic planning** – What impact will the crisis have on existing plans? Periodically update the organizational crisis team on the status of all "human and physical assets."
- **International** – Does local custom mandate burying victims within 24 hours? Must you confiscate passports of any potentially implicated employees?
- **Public affairs** – Do you need government or lobbying assistance? What are the organization's "fiduciary obligations" to investors?

"Ten Pillars of Business Continuity"

Your post-crisis push is to get back to business. For future stability, try these 10 best practices:

1. When disaster strikes, you cannot possibly over-communicate with victims.
2. Be in 24/7 contact with "employees, contractors and vendors."
3. Get your off-site IT recovery operations and EOC up and running as soon as possible.
4. Make sure the staff receives full salaries and benefits. Give the incident commander authority to pay for "equipment, hotel rooms and consulting services" as needed. Document everything, including damages. Plug in your insurance carrier ASAP.
5. One and only one spokesperson communicates. Employees should refer all questions to that spokesperson. Avoid policy infractions. Control rumors.
6. Designate psychological counselors and make them available for anyone affected.
7. Update stakeholders three times daily concerning all activities and progress.
8. Stay on top of all suppliers. Make sure they aid the recovery in a timely manner.
9. Make sure the disaster is over before you declare it done. Consider "scenario testing" to ensure that things are again as they should be. Plan a "multi-tiered return to normalcy."
10. Assess event fallout. Establish accountability. Reward anyone who deserves it.

About the Author

Laurence Barton, Ph.D., is a crisis management expert who has handled more than 1,200 crisis incidents worldwide. He is a management professor at The American College, Bryn Mawr, Pa.