# HOW TO PREPARE FOR THE CRISIS YOU HOPE NEVER HAPPENS

This tool explains how to prepare for a crisis that you hope will never happen. We can all think of examples of leaders who failed to react well when a crisis hit. Think about Watergate. Think about Arthur Anderson and the Enron scandal. Think about Ford Motor Company's failure to replace faulty tires on its Explorer SUVs. Nixon was forced to resign. Ford's stock price plunged. Anderson went belly up.

At stake in crises like these is nothing less than the fate of your organization. Even a relatively small crisis can cost your organization dearly if handled poorly. So understand what's at stake. Any event, no matter how small, can spin out of control and become a disaster.

Effective leaders know that they'll have to deal with a crisis at some point. They also know that the worst crises are those you don't see coming. Rather than pretend that it won't happen to them, they employ specific practices to plan for – and manage – a crisis. Your planning should include the following seven elements:

**1. Plan Different Crisis Scenarios**

To prepare for a crisis, you have to imagine all the worst case scenarios you can. Imagine hackers getting into your computer systems and wiping out files, or a gunman loose in your building, or people tampering with your products. Planning for the unexpected is much like preparing emergency plans for a natural disaster such as an earthquake or tornado. Every organization should list the possible crises that could befall it. There are seven categories of crisis:

> **Natural disasters**: These include storms, fires, earthquakes, epidemics, and interruptions of power. In general, the public will not blame an organization for any fallout from a natural disaster – unless human error or misjudgment compounds it.
>
> **Economic crises**: These include labor strife, labor shortages, major declines in share price, major fluctuations in earnings, and economic disruptions. This type of crisis is likely to be triggered by grave errors in judgment, so it will be tempting to try to cover up. Remember the trust-empathy matrix!
>
> **Information crises**: These include computer security breaches, breach of copyrights, breach of patent, and loss of confidential information. These can either be the result of criminal activity, internal error, or a combination of both.
>
> **Physical crises**: These include breakdowns in key equipment, disruptions of assembly lines, loss of key facilities. Again, these are typically the result of both internal error and external factors.

**Human resource crises**: These include loss of key executives or employees, and legal problems such as embezzlement or sexual harassment. These are typically self-made crises. Cover-ups are likely to occur in this area, so watch out!
**Reputation crises**: These include libel and slander, and damage to corporate reputation. These will already be exposed in the media, so a cover-up is not in question. What's in question is how to assume responsibility when the damage is self-inflicted.

**Criminal crises**: These include product tampering, bomb threats, terrorist acts, shootings on site, kidnapping, hostage taking, and other forms of workplace violence. Typically these require immediate action by police and other authorities – so you need to be prepared to work closely with them. At the same time, you need to expand your frame of responsibility and be prepared to launch broad protective measures.

**2. Have a Crisis Response Team in Place**

When a crisis hits, a response team must be ready to take charge. This crisis response team should be prepared ahead of time to assume responsibility. The team should be composed of people who are both senior in the organization and trained in how to respond. It needs to have a clear line of succession so if one person is not available, another can step in. In large organizations, this team may consist of five to ten individuals, including the chief executive.

**3. Develop Response Modules**

Once you've listed the possible scenarios, develop responses modules that can be combined and adapted for use in different scenarios. Preparing different modules will give the crisis management team greater flexibility and make it easier to respond quickly.

Individual response modules might include the following: go to back-up power, notify fire or police, quick evacuation, essential services only, lockdown the facility, and transfer to secondary location. A major fire might trigger "quick evacuation" and "notify fire and police." A different set of modules might be used to deal with a major interruption of power ("back-up power" and "essential services only"). A bomb threat might trigger "notify police," "quick evacuation," "lockdown," and "transfer to a secondary location."

Your particular industry will dictate the types of response modules needed. Make sure they're in place, well-rehearsed, and ready to go.

**4. Define Communication Protocols**

Each response module should define who's in charge and how they will communicate. Specific signals need to be established for various events. How severe is the crisis? (Many organizations use a three-stage system signified by codes yellow, orange, and red). How do you signal a decision to move from normal to "crisis" mode? How do you let people know that things are back to normal? Questions like these must be answered beforehand.

Pay particular attention to redundant systems of communication. What is the primary channel of communication? Radios? Cell phones? Are they compatible with other emergency responders? What's the back-up system? The crisis response team should work out these details in advance.

**5. Establish a Command Center**

The crisis response team needs a place where they can meet and coordinate their activities. Copies of the various response modules should be available. The center should have sufficient communications capacity (redundant power systems and redundant television, radio and internet access) to enable people to connect quickly. It should be large enough so people can congregate there without getting in each other's way. A backup command post, located some distance away, is also important.

**6. Have Resources on Hand**

Certain response scenarios require adequate reserves of food and water, backup power generation, fuel, and medical supplies. You may think you can negotiate these on the fly, but remember – it's going to be a seller's market. When a disaster hits, you'll be glad you're not out looking for food and clean water along with thousands of others.

**7. Run Simulation Exercises**

Every organization should test its crisis response plans at least once a year. These exercises should test the crisis response team's ability to adapt the response modules to a highly detailed scenario. After the exercise, people should be asked to evaluate what went well and what needs to be improved. Check the communications gear, command post, and tangible resources more frequently to make sure they're operational.

**Establishing Early Detection Systems**

After the World Trade Center attack on September 11, 2001, the FBI investigated what it had known about the hijackers. Research turned up a memo written by an agent in Arizona that warned of Muslim extremists piloting jetliners and evidence that Osama bin Laden wanted to "finish the job" of bombing the World Trade Center.

After the Challenger space shuttle blew up in January 1986, killing all seven astronauts on board, investigators went back to see what they could find. They discovered a string of internal memos warning about potential problems in the booster rocket O-rings. Management had ignored these memos. They had not deemed the evidence sufficiently convincing to justify spending hundreds of millions of dollars redesigning the booster rocket.

Detecting a crisis before it happens seems difficult, but in fact the principles of early detection are well known to intelligence experts. It's what smart leaders do to implement early detection systems that matters. There are three key steps in the process: 1) decide what to measure, 2) build measuring systems, and 3) establish an interdisciplinary monitoring team.

**1. Decide What to Measure**

You should be able to foresee what poses a significant threat to your business, your employees, customers, and key stakeholders. Things like accidents on the job, embezzlement, workplace violence, faulty products, interruptions of service and so forth.

By identifying threats in advance, you can avoid first reactions and jumping to conclusions. Often I've found a manager's first instinct is dead wrong. It's too tightly wound up in past experience. When a rogue trader at the Hong Kong branch of Baring's Bank began covering his losses with a trail of phony accounting, his superiors chose to ignore the signals that something was fishy. Essentially, they assumed that they could correct the situation. No one really wanted to confront what they were seeing. The rogue trader single-handedly caused the 130-year-old firm to go bankrupt.

In deciding what to watch for, don't rely on "lagging indicators" like customer surveys or media polls. Look at what really impacts your customers, and pay attention to that. One IT solutions company has a credo of "on time, on budget, and on spec." It closely monitors how well its teams perform in each of those three areas. And they know immediately when a team is off track.

**2. Build Early Warning Systems**

Once you know what to watch for, the next step is to build monitoring systems. Utility companies invest in "fault detection systems" that search for evidence of line breaks and send signals back to a dispatch office. In large banks, the accuracy of transactions is measured by sophisticated "neural networks" that search for irregularities. These artificial intelligence systems can learn as they search by identifying new patterns of normal versus abnormal behavior. They are constantly looking for new types of trouble, figuring that's where the gravest danger lies.

Early warning systems have to be tailored to your particular industry and needs. A retail grocery chain checks random packages for signs of spoilage and tampering. A large recording company keeps duplicate copies of all its recording contracts in an offshore vault. A law firm keeps redundant records of all its client files in an encrypted account on a special file server. A small business owner has her bank statements sent to her home instead of her work. "That way," she says, "everyone knows I'm monitoring the checks."

When you build measuring systems, avoid the temptation to assume that you can winnow out the improbable events and focus only on those that are likely to occur. Once you head down that slippery slope, you've effectively cut yourself off from the information that's going to help you most. For it's always the "improbable" event that will trigger the biggest crisis.

**3. Establish a Monitoring Team**

Once you know what you're measuring and how you're measuring it, a special team needs to monitor and discuss the information regularly. The team members should be drawn from various departments with different areas of expertise and should be led by

someone with strong management skills. Some people should come from the front lines so they can talk about what they're seeing and hearing from their customers.
The team may decide to set "threshold levels" for particular parameters to trigger heightened concern. It may decide to track certain trends until it gets a feel for what is normal. Whatever the case, the team should have the authority to raise red flags when it feels it is necessary. These red flags should go straight to the chief executive.

**Dilemmas of Crisis Management**

In times of crisis people can become overly deferential to the leadership. This creates a variety of thorny dilemmas. One dilemma is how to get dissident voices to speak up. When people are scared, how do you get them to speak their minds? A related dilemma is to sort out the truth and figure out whom to trust. As H. L. Mencken put it: "It is hard to believe that a man is telling the truth when you know that you would lie if you were in his place."

Effective leaders help prepare themselves to deal with thorny dilemmas such as these. One way is by using training simulations. Here's one fictional training scenario we've used:

A major chlorine gas leak has occurred at the Busfield Chemicals facility. Twenty employees and have been taken to the hospital. Three are in grave condition and not expected to live. The crisis team has met and evacuated the facility. All employees have been told to stay home until they are called back to work. The press has called the CEO, who is planning to issue a statement.

In consultation with his management team, CEO Marty Busfield has prepared a statement saying: "We're not sure exactly what happened, but our teams are investigating. My heart goes out to the victims and their families. I accept full responsibility for making sure our facility is safe before anyone goes back to work. We've shut down the plant and will not reopen it until tests are conducted to make sure everything is safe."

As the team nods their assent, the general counsel warns Busfield that his statement could set the company up for potential lawsuits. "By accepting responsibility, you're letting other people off the hook," he warns. "This may have been a faulty piece of equipment from one of our vendors. We need to launch a full investigation before we make such a public stance."

The VP of human resources speaks up. 'We do know that one of the victims had a history of not doing thorough safety checks. This may have been a result of employee error."

The general counsel chimes in: 'We're talking hundreds of millions of dollars in potential damages to people who may have suffered long-range damage to their health. Do you want to take that risk?"

Busfield pauses and then turns to you. "What do you think we should do?"

The exercise triggers lots of useful conversation. One of the best answers I've heard came from a young manager of a high-tech company in San Francisco. He said: "I would lay the situation squarely on the table by saying that while we need to consider how to protect ourselves legally, the bigger issue is protecting our reputation and goodwill. The statement says what we need to say. In the long run, we have to demonstrate our concern for people's welfare."

**How the California Earthquake Authority Prepares for a Crisis**

One of our clients is the California Earthquake Authority, a state-chartered agency that provides earthquake insurance to California homeowners. It's the CEA's job to prepare for the inevitable – a large, deadly earthquake in a heavily populated area of California. Paying claims to homeowners is the heart of the CEA's business. When a disaster strikes, the CEA strives to pay claims quickly. Its virtual network of agents must be able to ramp up quickly. Agents and adjusters must be trained to deal with emotionally distressed customers. CEA representatives must be able to go quickly to the scene to be available to answer any questions.

The very moment when the California Earthquake Authority most needs to handle calls and transmit data is the moment when such services are likely to be interrupted. The network of banks, insurance companies, adjusters, and other experts who make up the CEA need multiple, redundant ways of communicating. So twice a year the CEA runs stress tests on its lines of communication to make sure enough redundancy exists.

The third area of preparation is fielding questions from the public and the media. To prepare, all CEA managers participate twice a year in mock public forums. Communication experts toss out tough questions that managers and staff are expected to handle, and experts grade them on their responses. The sessions are videotaped and played back. All those who participate go through a rigorous personal evaluation of their strengths and weaknesses under fire – and are given specific areas in which to improve. Performance is rigorously monitored in real time and any mis-statements are quickly pointed out and clarified.

The CEA may seem like an extreme example. But in any organization, the same level of planning and rehearsal will help ensure a quality response.

**Conclusion**

A crisis is like a tsunami crashing into your organization. The better prepared you are, the higher the odds of surviving intact. Crisis response modules, early warning systems, and disaster drills are all part of smart leadership.

Leadership has to be prepared when a crisis hits. A single point of control needs to be ready to coordinate all the organization's activities. A different culture has to take over temporarily – a military-like command-and-control culture. Unless the culture is ready, cracks will appear.

In a time of crisis, your natural style as a leader will emerge. Some want to be hero-protectors. Others want to be self-sacrificing. Others try to deflect blame. Effective

leaders reframe their thinking and accept responsibility for whatever damage that occurs to customers, employees, shareholders and other stakeholders, regardless of who actually instigated the crisis. They display a calm, forceful quality; they work with the media, and are not stampeded into errors of judgment.

Long before a crisis hits, effective leaders build early detection systems and crisis monitoring teams. They also make sure they've built strong reservoirs of trust with key people in their organization so that when the inevitable crisis hits, they have people they can rely on.

A leader who survives a crisis learns a critical lesson: Crisis management is a lot easier when we put the broader needs of our customers and employees and the public first.