



**THE SEVEN BIGGEST MISTAKES YOU COULD MAKE  
WHEN BUILDING YOUR CRISIS MANAGEMENT  
PROGRAM – AND HOW TO AVOID THEM!**

A report prepared by COPE Solutions Inc.



## **THE SEVEN BIGGEST MISTAKES YOU COULD MAKE WHEN BUILDING YOUR CRISIS MANAGEMENT PROGRAM – AND HOW TO AVOID THEM!**

Most large companies understand that contingency planning and crisis management are essential activities in today's business climate. They know that an unplanned business interruption or crisis that spins out of control could mean disaster for the organization. Therefore, a significant amount of corporate resource is directed to developing crisis management programs. However, what management doesn't realize is that many of these programs are ineffective and that their organizations will not be adequately protected from the unexpected. Quite often, senior management believe that their company has a robust crisis management capability when, in reality, their company has been left extremely vulnerable because not all possible scenarios have been considered or incorrect assumptions have been made in terms of what is needed to handle specific crises.

### **Ineffective Crisis Management Programs Will Exhibit One Or More Of The Following Seven Mistakes:**

#### **Mistake #1 - Poor Planning Basis**

Most companies have Business Continuity Plans in place that are designed to help recover essential business operations following a disaster. For example, a company's critical data is protected through the establishment of hot sites and routine offsite data storage as backup. According to a survey conducted by Price Waterhouse Coopers, 85% of businesses in the financial services industry have disaster recovery plans. However, the same survey also indicates that only 15% of those businesses have fully conceived Crisis Management Plans. The question then becomes: How well prepared are the other 85% if they are faced with a crisis other than technology failure, such as a natural disaster, or a targeted boycott by a well-organized protest group, or perhaps a traumatized work force due to work place violence?

A Business Continuity Plan is only one component of a Crisis Management Program. Unless a company has considered all potential threat events, it will not be fully prepared to handle the full range of potential crises. An organization should not be lulled into the belief that they are vulnerable only to the obvious scenarios for their industry. For example, a European publishing company did not consider they would ever have to deal with the liability of consumers getting sick because they were using their encyclopedia. (During the publishing process, the captions that identified good mushrooms from poisonous ones were somehow reversed, thus identifying the poisonous mushrooms as edible!)

**Solution:** It is neither practical, nor realistic, that every potential scenario be planned for in detail. However, a company can avoid a poor planning basis in its Crisis Management Plan by conducting a thorough Threat Risk and Vulnerability Assessment. Identifying and recognizing all potential event types can achieve a solid planning basis.

Event types can be grouped as follows:

- Environmental (e.g. natural or manmade disasters)
- Technological (e.g. hazardous materials, design error)
- Human Threats (e.g. vandalism, insider trading, protest group actions, boycotts, criminal activity, terrorist attacks)
- Public Relations and Reputation issues

By addressing these broad categories, it is possible to develop the correct, viable planning basis for all potential event types, regardless of the specific scenario. This will, in turn, support development of crisis management capability.



### **Mistake #2 – Non-Systemic Approach to Crisis Management**

Many organizations have a Disaster Recovery Plan; and a Security Plan; and perhaps, a Crisis Communications Plan. But all too often, these plans are not integrated. There is no built-in mechanism or authority to coordinate them during a crisis event. To try and cobble together a coherent response protocol from numerous independent plans prepared in isolation is an onerous task. By preparing these plans independently there is significant risk of incorporating overlapping actions or duties and/or omitting key activities.

**Solution:** The way to achieve a comprehensive response capability is to develop a high-level Concept of Operations, which is derived from an all-hazards approach to crisis management. Once developed the Concept of Operations would then be reviewed with all stakeholders to ensure high-level acceptance. Only after receiving stakeholder support can a fully integrated Crisis Management Plan be developed. The plan may then include any of the sub-components: Disaster Recovery Plan, Security Plan, Crisis Communications Plan, etc. but all would be linked and coordinated based on the Concept of Operations.

### **Mistake #3 - Disconnected Response Team Operations**

Consider this example: A bomb threat states that a device had been placed in the corporate headquarters server room. Your security staff would want to conduct a controlled search of the area to verify if the threat was real. However, your Disaster Recovery Team would be rushing to the server room to commence procedures for linking to the company's back up site, while at the same time, the Facility Emergency Response Team would be evacuating the areas in the vicinity of the bomb. The Corporate Crisis Communications Team would be preparing an immediate news release stating that everything is under control, while the Crisis Management Team's legal counsel may advise that nothing is to be released until the liability ramifications have been addressed. Which team takes precedence? Who is in overall command? Do the various responders acknowledge this?

**Solution:** To avoid the potential chaos which would naturally ensue from the above scenario, the Crisis Management Plan needs to be developed from a sound, all-hazards planning basis and this process must involve all stakeholders. A rugged command and control structure needs to be in place that will clearly identify the chain of command, the level of authority at each command level within the organization and the process for transferring command between different levels as the scope of the incident expands or contracts. Finally – a regular exercise program that allows scenarios to be practiced will provide a learning opportunity for the Crisis Management Team and allow procedures to be validated before they are needed in a real scenario.

### **Mistake #4 - Response Team Lacks Authority**

When the Exxon Valdez ran aground and started spilling oil into Prince William Sound in Alaska, the initial response of Exxon Corporation was literally, almost nothing (beyond a news release claiming the environmental damage was minimal). The company didn't have a crisis response organization with the authority to undertake the situational assessment and make the timely decisions necessary to mitigate the crisis. Exxon paid a huge price for this (it has been roundly condemned for its initial reaction) and the CEO was eventually replaced. What's the lesson to others? Many companies have not designed their crisis response organizations with the appropriate authority to deal with a crisis. Often, the decision-making lines of authority and procedures are identical to normal line operations! Without the proper authority, the Crisis Management Team will be ineffective and will not be able to ensure the correct response to a crisis.



**Solution:** This can be overcome by implementing two protocols. Firstly, the Crisis Management Organization must have an up-to-date, and real time, alerting process that will activate at a moment's notice to ensure that all key members have been informed of the situation. (Many programs do not have these procedures in place.) Secondly, a clear command and control system must be designed that allows decisions to be made immediately in responding to an event. This decision-making authority must take precedence over the normal line organization and must transcend all functional areas of the company and business units. The response will fail if the leader of the Crisis Management Team does not have full authority to coordinate and direct the activity of any function of the organization he requires. His authority, and that of the Crisis Management team, must be clearly defined beforehand to ensure all elements of the organization understand from whom they must take direction.

Jurisdictional disputes and internal political arguments have no place during a response to crisis since they could exacerbate an already dangerous or difficult situation. A clear command and control protocol is vital in avoiding these problems.

### **Mistake #5 - Ineffective Operational Documentation**

It seems obvious that an emergency response plan should be the essential tool for the personnel responding to an event. Too often, this is not the case. Plans are generally inches thick and written more to protect the author and/or the organization than as a tool to assist the response teams. On September 11, 2001, many government crisis management plans were opened for the first time in years. In one case, the first sixty pages dealt with the legislative and organizational justifications for that particular department's responsibilities. As a document for providing direction to the crisis management responders, it was useless. Many private corporation plans also exhibit these characteristics.

**Solution:** Crisis Management Plans should be designed and written for the people that need to use them. As a general rule, they should define the Crisis Management Organization and the roles and responsibilities of key players. Communication protocols and information management should also be covered. And that's it! Planning and program rationale and situation specific procedures can be included in appropriate appendices, but if the main document is much over 25 pages, it probably contains unnecessary information and will not serve the responders as well as it could. By keeping it concise and limiting the information to the direction the Crisis Management Team needs to take, the documentation will be focused and an excellent tool during an emergency response.

### **Mistake #6 - Program Not Kept Up-to-Date**

Another common mistake is not keeping the Crisis Management Plan and response team training up-to-date. Many companies expend considerable resource (both in financial terms and in employee time) to produce a plan that is then put on a shelf and forgotten. Consider the case of a rail transit authority participating in a municipally sponsored disaster exercise. The scenario involved a train hitting a tanker truck at a road crossing, resulting in mass casualties and an environmental problem. When the transit authority's response plan was opened up, responders found that all of the alerting information was out of date by as much as three years. Office numbers and contact information were incorrect and key crisis management personnel could not be located. The contact number for one of the designated on-scene incident commanders turned out to be an obscure maintenance office. Further, the majority of the Crisis Management Team members had not received adequate training, if any, for their roles. Crisis training had been conducted in the past, but many personnel had since moved to other positions or left the Transit Authority altogether. Even the ones that had received some training could not cope during the simulation because they had lost these perishable skills. The exercise proved that they had no



crisis management capability, although senior management honestly believed that it was in place and the organization could protect itself in the event of crisis.

Another characteristic of crisis response plans is that they are often based only on what has happened in the past – not what could happen today. Plans and procedures must be adapted and amended as the world changes. In previous years, companies may have had a few hours to consider a public response to an incident before having to make a statement. Not today. With the evolution of media communications and proliferation of the internet, organizations now have to answer questions, literally, in minutes. A company's crisis management capability must reflect this requirement. With today's technology, and the increasing sophistication of criminal and terrorist groups, security plans have to rapidly evolve and change in order to meet current threats.

**Solution:** By implementing an ongoing plan review and training system, crisis management capabilities are easily sustainable. Organizations must realize that crisis management planning is not a one-time exercise. It should be viewed as an ongoing program and, if done properly, the capability can be sustained perpetually. Sustainability does not have to represent a huge allocation of resources. In fact, keeping a plan current and valid through routine maintenance is significantly cheaper than rewriting a new plan every two or three years. By reviewing plans semi-annually and checking basic components such as notification lists, crisis management team equipment and facilities, plans will remain valid and will not require rewriting. Personnel training programs also need to be kept current and teams need to be able to develop and practice their skills. This is particularly important as personnel move into different roles or are replaced with new faces. It is also necessary because the skills required to make a Crisis Management Team function properly are perishable. They must be practiced regularly.

#### **Mistake #7 – Lack of Crisis Leadership Skills**

Perhaps the most common mistake made by the senior personnel of an organization in preparing to face crisis is assuming that they have the leadership qualities to make the necessary decisions during a crisis situation. Many corporate leaders believe that if senior managers are required to direct people and make decisions on a daily basis, no specialized training is required during a crisis – they already have the leadership skills to make the right decisions, regardless of the size, scope and nature of the situation. What is so different about running a crisis management response team than running a business unit?

A case in point: In the Winter of 1998, Quebec Hydro was crippled by an ice storm that destroyed a good portion of the electrical grid and left hundreds of thousands of people without power. When the rain stopped, the devastation was on a scale unlike anything ever seen in North America. It was obvious that immediate decisions were needed in order to start reconstruction and to get power back to a population having to survive without heat. However, the leaders of the corporation were incapable of making any of the required decisions. The organization had no real crisis management capability and none of the senior personnel had ever been confronted with a situation of this magnitude. They could not prioritize or adequately assess the massive problem they faced. It was only with military assistance that the proper prioritizations and resource allocation decisions were made.

In any crisis, the challenge faced by the senior decision maker is the need to make timely decisions in order to gain immediate control of the situation. However, there is often incomplete information available upon which to base decisions. Contrary to the typical business decision-making process, the luxury of time to collect relevant data, to develop and compare various options and then to select the best course of action is simply not available.



Decisions need to be made urgently and those decisions often have the potential of grave consequences. The outcome of a crisis is often determined by the decisions made in the initial stages of the incident. If these initial decisions are wrong, then the whole response will often be a disaster.

**Solution:** Crisis leadership and effective decision-making in a crisis can be developed. Through practical and specialized training, the process of decision-making during crisis can be systemized. Decision-makers can be exposed, beforehand, to the stresses of making immediate and far reaching decisions based on less than complete information. By establishing and ingraining the corporate value hierarchy in the decision-makers (such as safety of personnel, safety of environment and asset protection), a decision tree can be developed that supports appropriate decision making regardless of the event. Leadership in situations of high stress can also be developed. A crisis is not a time for a business oriented management style. It will involve some regular management skills, but also dynamic leadership and when necessary, Command. Crisis is not the time to pass the buck or spend more time than you have looking for suggestions and consensus. Successful companies select Crisis Management Team leaders not only in terms of his/her position or seniority in the organization but also based on leadership and decision-making ability.

