

Experience tells us that it is best to compile this information within a relational database software program. As the needs and expectations of the various functions change within the organization, it will require a software program to keep track of how each change will affect myriad others throughout the organization. Ask someone from your IT department or a software consultant about applications that would be best to integrate the needs and expectations of your various departments for each foreseeable risk.

**Without clear guidelines about the strategic direction of the response, communication channels, and limits of authority, the crisis response can lose focus quickly.**

## 12.4.2 Integration Failure Points

In my experience over the years of assisting crisis management teams, I have noticed three areas that seem to cause problems repeatedly during crisis responses. The acronym ACE (Authority, Communications, and Expectations) may help you remember these important areas where your crisis teams could run into difficulties.

- ▶ **Authority.** During a crisis is not the best time to determine who has authority for important decision-making. A common failure point occurs when individuals do not assume authority and responsibility when it is expected. When people are not fully empowered with clear boundaries and guidelines, they have a tendency to back away, especially when important decisions need to be made based on only vague guidelines about what is the best action to take. The default actions are avoidance or delay in order to obtain guidance from an appropriate superior. If authority is not assumed at appropriate levels, precious time is lost, and the effectiveness of the crisis response is compromised.

The converse is also problematic. In this case, individuals assume positions of authority without prior approval. This can result in a crisis response situation where decisions can be in conflict. Without clear guidelines about the strategic direction of the response, communication channels, and limits of authority, the crisis response can lose focus quickly.

It is critically important that appropriate individuals know they are to assume authority at defined levels. Thresholds should be clearly established to enable individuals to know the limits of their authority and at what point they need to garner approvals from superiors.

*Prearranged authority* is a concern with companies that use the incident command system (ICS) within a corporate setting. ICS is a subcomponent of the National Incident Management System (NIMS), as released by the US Department of Homeland Security (DHS) in 2004. Many companies use it successfully; others end up in a quagmire of conflict. ICS assigns an incident commander with authority over the entire crisis response. However, a problem area emerges because the incident commander is seldom the CEO of the organization and many times the incident commander is not on the leadership team.

The conflict with authority comes when the incident commander orders a response to a higher ranking manager in the company. During normal times, this would never happen. And, if that ranking manager disagrees with the incident commander's decision, a conflict of authority breaks out in the midst of fast-moving, high-consequence crisis events. Such a conflict can slow down the response, create noncompliance, send mixed messages, and undermine the crisis management structure within the organization.

Even without the ICS system, managers need to know the boundaries of their authority. At what point does our plant manager with the facility fire need to defer to business units heads or corporate management for decisions? Often, for example, the plant manager could give prepared holding statements to the press, but any incident-specific statements to the media would have to be approved or provided by corporate.

- **Communications.** No crisis response is any better than its communications. The most fundamental building block of any relationship is communication (whether crisis related or in daily living).

Engaged crisis teams must receive good information in order to assess the situation and contain the damage. Likewise, they must give out good information to involved stakeholders in order to orchestrate a unified and effective response.

Timely and accurate two-way information should flow between crisis managers and appropriate internal and external stakeholders. Depending on the incident, communications can be compromised with power outages, run down batteries, generators running out of fuel, attorneys with liability concerns attempting to limit transparency, inoperable or overloaded mobile phone towers, overloaded landline phone systems, email that may not work, rumors, misinformation, misunderstandings, fear of disclosure, employees and others speaking without authority, social media, and other impediments. Good planning should include contingencies for these occurrences.