Managing

BY MICHAEL BLYTH

How to Handle a Crisis

Managers must train employees, develop protocols, and design record-keeping programs to ensure a solid response during a crisis.

NO ONE CAN PREDICT when a crisis will hit, but it's security's job to be ready whenever it does. The key is a good plan. A good crisis management plan includes developing and staffing well-organized teams, establishing response protocols and report templates, designing recordkeeping policies, staging postincident reviews, and maintaining monitoring programs.

Teams

The crisis management team should consist of three layers of management: a corporate crisis response team, a country crisis response team, and a program crisis response team.

Corporate team. The corporate team will have overall crisis resource mobilization and coordination decision-making authority and will be responsible for strategic planning considerations and liaising with senior-level government officials.

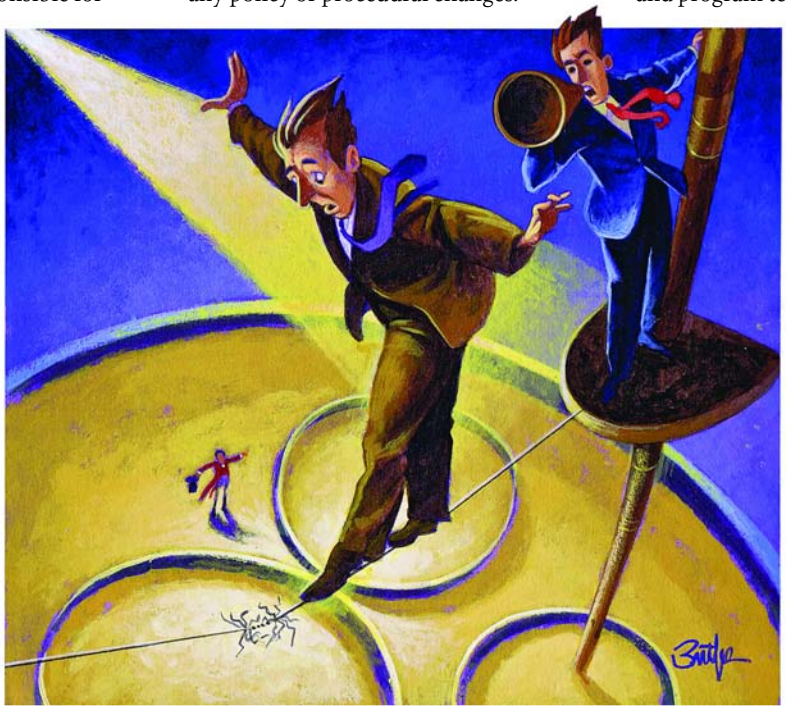
During the incident, the corporate team will liaise with any vendors to ensure that all appropriate measures are being taken in terms of operational support and business continuity.

The security vendor's corporate team should also ensure that close support is offered at corporate levels throughout the crisis event, providing all of the information and documentation requirements.

In addition, the corporate team will ensure that the human resources, media, and legal groups of every party involved, including vendors, coordinate the release of information. Most important, the corporate team will ensure that information is shared with employee families and that anyone involved in the incident gets the appropriate care and support.

The corporate team will typically mobilize all HR, media, government, and legal specialists to offer support, guidance, and management of personnel.

Following an incident, the corporate team will be responsible for capturing all information, not only for use during the incident but also for use in conducting an audit of the incident. That will ensure that lessons learned can be analyzed for any policy or procedural changes.



Country team. The country team consists of the most senior managers responsible for a geographic region, typically led by the country manager or general manager. Companies with operations in only one country can eliminate this team. In these cases, the country team's responsibilities will often be performed by program teams.

The country team coordinates all national-level activities and serves as the focal point of the company's crisis management efforts on the ground in that locale. The country team has the local expertise and relationships to mobilize resources and support in that country to deal practically with an incident on behalf of and under direction of the corporate team.

The country team provides expert advice and recommendations to both corporate and program teams and also coordinates all support in the area from both internal and external resources, including military, diplomatic, and other supporting organizations.

This team also focuses on information flow from the program team to the in-country security vendors and teammates.

Program team. The program team is led by the most senior corporate security executive or outside consultant within each country for a particular business activity or unit. The program team manager ensures that all security

continued on page 99

ILLUSTRATION BY RALPH BUTLER

continued from page 100

staff and supporting military, medical, and other external service support are directed to assist the local incident response team commander to effectively extract personnel and assets from the risk area.

This team ensures that any medical support is readied to receive casualties. In addition, the program team often integrates any vendor staff, such as security guards, into the existing program team to ensure that they complement each other's efforts and avoid duplication.

The program team's secondary function is to notify all company management chains of the incident to initiate country and corporate crisis management structures. At appropriate junctures, the program team manager will provide detailed updates as well as formal incident reports. The program team typically reports directly to the country team, which in turn reports to the corporate team.

Each of these teams should have a range of personnel with the skills required to analyze and deal with these events, from the management or command elements to specialist advisors. Hierarchy and politics should not be an aspect of management selection. Responsibilities should be assigned based on competence and experience.

The role of the crisis management team is to be in a position to respond effectively to postulated threats or actual events in a timely manner. Management commitment is critical for the success of the program.

The crisis management teams should flow information and recommendations up to the corporate management or executive board while having decision-making autonomy within certain parameters.

The level of decision making, responsibility, and authority will vary depending on the corporate structure. Generally, however, managers should consider staffing each team with the following members: team commander, administration manager, intelligence or information officer, physical security manager, technical security manager, liaison officer, crisis communications manager, public relations officer, legal counsel, stress trauma advisor, reception team manager, and finance officer.

Team members must be trained along with all company employees to ensure that all participants understand their roles during a crisis. For example, because the finance officer is involved with the money side of the equation, he or she must be trained in what sorts of funds are available during a disaster and who should be authorized to draw on those funds. Also, all employees should have contact sheets with the names and phone numbers of important people, such as bomb technicians, hospital contacts, and government officials.

Policies and protocols. The types of risks a company may face can be determined prior to an event, although the scope and unique peculiarities will change on a case-by-case basis. Pragmatic crisis management protocols should be developed to support management structures in dealing with the initial effects of an emergency, reduce the initial and subsequent impacts, and bring some degree of control to the event. Protocols also provide a handrail for less experienced managers to guide them through decision making and information gathering, offering direction and confidence during the early stages of an event.

Report templates. As part of the crisis management protocols, employees should also learn how to use crisis-management report templates. These templates provide basic guidelines to employees on how to report an incident. If managers design these templates effectively, employees will only need to fill in the blanks to provide the right information.

These templates should ask for data such as the date and nature of the incident, how many people were injured, what type of damage or loss was incurred, the names of those involved, and what mitigating action was taken.

Record keeping. Information in the report templates becomes part of the official record of the crisis. This documentation is used in any subsequent government or civil audits, employee issues, and insurance claims, for example. In addition, this information is critical for learning from a crisis and protecting against any ramifications arising out of the incident.

Lawsuits against the company, for example, can surface months or even years after the crisis. Those involved in the crisis might have faulty memories, and many key players may have moved on to different jobs, making an accurate defense difficult absent good records.

Postincident review. Following any incident, the company's crisis management teams should conduct a detailed debriefing at all levels of the company to ensure that mitigating procedures were fully implemented and that any follow-up requirements were met.

For example, following the evacuation of a site due to severe weather, the company might review whether the facility was correctly secured and what damages to infrastructure might have been avoided. In addition, the success of any methods of remote business operations, such as telecommuting, might be evaluated based on the ability of management to operate without power or utilities.

The purpose of a postincident review is to address gaps that might hinder operations in future crises. For example, the company might review whether management and site staff were correctly trained in the existing policies and plans as well as how their ability to respond confidently and effectively might have been enhanced. If gaps and shortfalls are identified, training may be a logical remedy.

Monitoring. The crisis-management teams must keep the protocols and records current. Training and contact information should be updated, team members should be briefed on changes in the company, and threat assessments should be altered to reflect evolving geopolitical realities.

Companies must monitor fluid risks, especially man-made threats such as crime and event-driven risks such as rallies or protests. Companies should review the types of risks and how these might change or evolve over time. Policies and plans may need to be periodically adjusted to address changes.

Companies are constantly at risk of an incident that may create a crisis. Whatever the nature of the situation, however, an established, organized crisis-management plan can help the business respond appropriately. ■

Michael Blyth is director of risk consulting for BSG LLC based in Washington, D.C. He is author of *Risk and Security Management* published by John Wiley & Sons.