



CRISIS MANAGEMENT PLANNING

Approach crisis management challenges with the right knowledge tools

by Randall R. Nason

In spite of our best efforts to strategically apply every piece of technology available and all best practices, eventually every organization will experience a crisis of some magnitude. At that point, regardless of the initiating event, the most important goal is to recover the business as quickly and as cost effectively as possible.

We in the security industry know all about crisis avoidance and prevention. After all, the primary thrust of our jobs is to implement a program that will prevent or deter unacceptable behavior directed at our organization. And it is within this context that security and crisis management become adjacent, and in some circumstances, overlapping functions.

The two functions are adjacent in that certain classes of threats must pass through the security program to cause a crisis impacting the organization. For example, a disgruntled former employee must bypass technological, procedural and administrative security controls to regain access to a corporate facility and take a hostage. Crisis management

takes over after the threat “defeats” the security program. However, these functions overlap as well, since security would play an ongoing role in resolving the crisis.

The strategic response to a potential organization-threatening crisis is the crisis management or emergency operations plan. In broad terms, the strategy is to prevent or avoid the initiating event, mitigate the consequences of the event should it occur, and recover from the event as quickly as possible.

The Goals of Crisis Management

The goals of an organizational crisis management plan are clear and well known¹:

1) Define the crisis in terms that are applicable and understandable to the organization. Different organizations face different types of crises depending on their

1 Asset Protection and Security Management Handbook, POA Publishing LLC, Auerback Publications, a CRC Press Company, New York, New York, 2002.

focus, location, ownership structure, position in their industry, threats faced, and level of preparation. Carefully defining in real terms the family of crises that could threaten the very existence of an organization helps to elevate the importance and practicality of the plan development effort.

2) Establish an organization to deal with the crisis immediately before and during the crisis, as well as during the recovery stage. These individuals need to be a special breed that can make strategic decisions in the midst of what may be chaotic circumstances and with much less than adequate information.

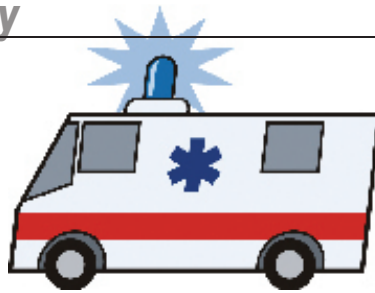
3) Establish procedures for quickly accessing internal and external resources as needed. During times of crisis, normal procurement channels will be unacceptable. Those involved in crisis management need access to the necessary recovery tools immediately. Additionally, the normal chain of command may be unworkable. Key individuals may be unavailable; communication paths may be unreliable and slow; if the crisis is brought on by a natural disaster, available supplies may be dwindling due to demand by all organizations in a particular region.

4) Establish benchmarks to signal when the organization is ready to move out of emergency operations and back to some level of normalcy. The emergency operations mode is not an efficient business model. Established metrics can help signal the crisis management team to begin the transition back to normal operations.

Planning Isn't Just Long-Term

Crisis management is all about planning. This planning is normally subdivided into five categories: long-range planning (the event is not in sight), near-term planning (the event, such as a hurricane, is expected in two to three days), event planning (the crisis is ongoing), response planning (short-term response actions after the event has occurred), and recovery (late response actions and transition to normal operations). This list clearly recognizes that there is much an organization can do to prepare for a crisis.

In general, any contingency that can be defined in terms of an initiating event with subsequent consequences



In reality, the crisis management plan is an ever-evolving document that changes as personnel and response strategies change.

can be the object of long-range crisis management planning activity. Events that lend themselves particularly well to this type of approach include weather (tornados, hurricanes, ice storms, floods), fire, power outage, water outage, communications failure, bomb threat, HAZMAT incident, and computer system failure. Other types of incidents can also be the object of long-range planning; however, these incidents are, in some respects, less frequent and are inherently more variable than the incidents above, with which we are much more familiar. This latter category includes explosions, workplace violence, hostage incidents, and social unrest or civil disorder.

Universal Crisis Management Problems

There are several common problems in organizations' crisis management programs today.

First, many organizations do not have a formal crisis management plan or structure with which to begin to prepare for or respond to a crisis event. In many organizations, ongoing business activities easily consume the available staff resources. Unfortunately, this organization will not have even a basic structure for response when an unexpected event occurs.

While the argument can be made that every business cannot afford to put off crisis management planning, those businesses with limited resources should at least assemble a basic planning and response docu-

ment. This document at a minimum should contain contact information for those individuals designated to be in charge in the event of a crisis. This basic structure will provide a starting point.

Second, many organizations view their crisis management as a completed document; as such it sits on the shelf in various locations within the organization. If it is needed, the right people know where to find it.

In reality, the crisis management plan is an ever-evolving document that changes as personnel and response strategies change. At a minimum, awareness briefings should be provided to those individuals with crisis management responsibilities to provide the foundational information necessary to begin to deal with a crisis event.

Third, there is little training of the staff with regard to translating the crisis management plan guidelines into action. This can only be accomplished through various table-top exercises or full-scale simulations.

Challenges for Enterprises

The development and maintenance of a corporate crisis management plan is often complicated by the geographical and functional diversity of an organization.

- First, most organizations find it difficult to dedicate the necessary resources to develop a core crisis management plan. Under the enterprise model, a crisis management plan may need to be developed, or at least tailored to each major facility in the portfolio. Under these circumstances, organizations should provide as much commonality as possible in the core crisis management plan; the distributed facilities would then only have to modify the external support agencies' emergency contact lists to fit their particular location. While this places the burden of crisis management planning on corporate shoulders, this is normally where these resources reside.

- Second, because of potential functional and geographical diversity, the range of potential crisis types faced by the organization at large can be extensive.

Again, corporate-level planning should take into account this diver-

What Legislation, Regulations and Voluntary Guidelines Affect Your Organization?

Few security professionals are familiar with all of the laws and regulations that have placed security requirements on corporations since 9-11. Even fewer are aware that laws and regulations concerning computer security, business conduct and ethics and privacy all have security elements to them.

Security has gone from one of the least-regulated to the most-regulated staff group in the corporation. What we once thought were good, voluntary practices may now be required. The consequences of noncompliance can now carry fines, corporate image damage and even jail time for those responsible.

Every sector has regulations and agencies requiring security measures. One review identified 78 federal agencies alone claiming some responsibility for food safety and

security, for example.

Increasing regulation will impact business continuity and security's overall cost to business. And what if there are duplications, inconsistencies, or conflicts among regulations from different agencies and organizations?

What is the new role of security in this environment? Which staff group has the lead—legal, compliance, risk management, IT security, corporate security, supply chain, human resources, internal audit or executive management? What responsibilities will corporate security have? How will we make everyone aware of all of the issues?

In collaboration with the Security Executive Council (SEC), *ST&D* will now feature a regular update in this column to help you stay abreast of the regulatory changes, their impact, and

effective strategies for addressing them.

The SEC has created a database of security laws, regulations and industry voluntary compliance programs (LRVC), but there are more out there that aren't yet in this library. Send copies, Web sites or links for regulations impacting your organization to cso_ec@cxo.com. For submitting new LRVC information that is not yet on their list, the SEC will send you a complimentary metrics slide that retails for \$50 from its Presentation Library on Communicating Security Value to Senior Management.

Check back in April for the first compliance scorecard. It's information you can't afford to miss. **ST&D**

The Security Executive Council is online at www.csoexecutivecouncil.com/?sourceCode=std.

The Business of Security

sity and provide the necessary core response structures to address all hazards. Local tailoring with corporate support will provide the local information and strategy needed for local applicability.

Third, identification and coordination of support from local agencies, such as law enforcement, will need to be done locally. The corporate crisis planning team will need to ensure that these relationships are in place.

• Fourth, depending on the event, the local crisis management team could need anything and everything from office supplies and building materials to rental cars, computers, and two-way radios. While some of these needs could be foreseen and accommodated through a corporate account with a national supplier, actual supply of the items would most likely need to be local. Experience has shown that establishing *a priori* local sources of necessary

supplies is a necessity.

• Finally, enterprises need to be particularly careful to coordinate the flow of information. Many crisis management guides stress the importance of managing the information provided to interested and affected parties, including employees, families, stockholders, and the media. Individual facilities may not have an individual designated or trained to interface with the press. The corporate public affairs person may be thousands of miles away at the corporate headquarters with second-hand information. This difficulty must be planned for in advance in order to ensure a clear and correct version of the event is conveyed to all parties.

One of the most important ways to improve your crisis management plan is to practice. The familiarity with the plan brought about by practice will enable your team to come to quick decisions about cri-

sis responses and be able to efficiently access the resources necessary to protect the organizational assets, both staff and capital. In next month's issue, I'll discuss how to organize and conduct an effective crisis management exercise and how to use the resulting information to improve your program. **ST&D**



Randall R. Nason, PE, CPP is a corporate vice president and manager of the Security Consulting Group at C.H. Guernsey & Co.

His experience spans a broad spectrum of the security profession including threat assessment, vulnerability analysis and master plan development through complete system design and construction management.