CRISIS MANAGEMENT

The Art of Crisis Management

While we do not propose a formal definition of the word *crisis* in this manual, we treat any event that can, within a short period of time, harm your institution's constituents, its facilities, its finances or its reputation as a *crisis*.

Crisis management is the art of making decisions to head off or mitigate the effects of such an event, often while the event itself is unfolding. This often means making decisions about your institution's future while you are under stress and while you lack key pieces of information.

Consistent with the overall philosophy of this manual, the key to being able to manage a crisis is doing as much planning as practical before a crisis starts in order to best position you and your institution to respond to and mitigate such a situation.

The Crisis Management Continuum: Introduction

What is usually called "crisis management" should be best understood as part of a broad continuum of activities as follows:

- **Planning.** Planning relates to getting your institution in the best position to react to, and recover from, an emergency.

- **Incident Response.** Incident responses are the processes that you have put into place to ensure that your institution reacts properly and orderly to an incident as it occurs. Examples of incident response include:
    a. Evacuation after a called-in bomb threat
    b. Denial of entry to suspicious persons
    c. Calling for medical help when a child is injured in your school

- **Crisis Management.** Crisis Management is the management and coordination of your institution's responses to an incident that threatens to harm, or has harmed, your institution's people, structures, ability to operate, valuables and/or reputation. It takes into account your planning and automatic incident response, but must also dynamically deal with situations as they unfold, often in unpredictable ways.

- **Business Continuity.** Business continuity relates to those steps necessary to restore your institution to normal functioning.

As will be discussed in detail below, a great deal of crisis management occurs before a crisis begins: it is about planning and preparing.

The Crisis Management Continuum: Planning

Introduction

As mentioned above, planning relates to getting your institution in the best position to react to, and recover from, a crisis. Planning for a crisis is discussed in some detail throughout this manual. For example, the chapter on explosive threats helps you consider what is necessary to plan to respond to an explosive threat-related crisis at your institution. The chapter on armed intruders seeks to do the same.

However, there are two elements of planning that are unique to managing a crisis:

- *Creating escalation rules for your employees* and
- *Creating a crisis team.*

In short, the goal is to have **employees who know when to report problems** and **a team of senior employees who are ready to react to them**. Each will be discussed in turn.

Creating Escalation Rules for Your Employees: Preventing, Detecting and Controlling a Crisis

Creating escalation rules for your employees is an essential element in crisis prevention, detection, and control. This means that you train your employees to bring matters to the attention of more senior personnel for their analysis and handling as soon as possible, preferably before they become critical. It means not only setting clear rules for when an employee must notify senior staff of a problem (for example, whenever a caller or letter writer mentions suing your institution), but also empowering staff to feel comfortable reporting concerns to senior staff (for example, ensuring that junior staff do

not feel at risk of ridicule or a negative job review if they in good faith report what they inaccurately believe is a problem).

Without such rules, a developing crisis may go unnoticed by senior management until it develops, appears in the press, and/or turns into a calamity.

- Choosing to Act — or Not

Creating escalation rules is important because when and how a manager becomes aware of a crisis can often determine how an institution responds — and how successful it can be in its response. Consider these two scenarios:

1. A synagogue employee receives a phone call that, while not overtly threatening, is a rambling speech that contains some very anti-Semitic remarks. The employee doesn't inform the director of the call. (Institutional discussion of situation ends)

2. A synagogue employee receives a phone call that, while not overtly threatening, is a rambling speech that contains some very anti-Semitic remarks. After the call, the employee makes a note of all the information relating to the call, informs his/her supervisor (the synagogue director), who in turn calls the police to file a report. Afterwards, after consulting with the synagogue President, he/she decides that the situation warrants extra security during the upcoming high holidays and briefs security personnel accordingly.

Clearly, the two institutional responses are very different. In the first case, because the clerk did nothing at all, management was simply cut out of the decision making process. Had the employee escalated because, say, the synagogue's management had instructed its employees to draw to management's attention such an unusual occurrence, the management of the synagogue would have been able to react or consciously choose not to react. Simply, without an escalation rule, an institution's management may lose a critical opportunity to react.

- When to Escalate?

The key question is what should cause such an escalation? How should an institution handle the task of teaching its staff and volunteers to know when to escalate?

There is no science in creating such a plan and the institution's leadership should think

about the kinds of incidents they would want to know about immediately. These may include, but are not limited to:

1. Security threats (e.g., bomb threats)
2. Allegations that may expose the institution to legal liability or embarrassment
3. Allegations that an employee or lay volunteer is acting in a manner that is inconsistent with the institution's best interests, such as misuse of an institution's resources
4. Any inconsistency between expected and actual bank balances
5. Requests for information that is inappropriate (i.e., a request by an unknown person for an employee's home address)
6. Requests for information relating to the institution's security or infrastructure (i.e., a request for information about where employees park or when the office is unoccupied)
7. Requests for donor information
8. Attempts to improperly access computer systems and/or "hack" an institution's Web site
9. All other contacts that concern the employee
10. All unusual events, including repeated hang-up phone calls, calls that contain sharp disagreement with an institution's policy or practice, and visitors who concern the employee

The institution's leadership should create a reporting mechanism (e.g., a log) to maintain a log of these and other incidents.

Of course, many of the above may be consistent with lawful and innocent behavior and a good deal of judgment and discretion is required. Finally, this is not a complete list, and such a list must be drawn up with your particular institution's situation in mind.

Management must work to create a culture where employees can communicate these incidents to management's attention without fearing overreaction or any negative consequences to the reporting employee (including feeling as if they are not being treated seriously).

Creating a Crisis Team

A second key element of getting your institution in the best position to react to, and recover from, an emergency relates to the creation of a crisis team that is ready to quickly come together to help manage an institution's way through a crisis.

The senior manager of an institution should establish a mechanism for pulling together a crisis team. She should:

1. Identify the key players who will be on a crisis management team, based on their specialties, willingness to serve, and personalities

    a. Example (large institution): Senior manager, Board Chair, Rabbi, Facilities Chair, Principal, General Counsel, Information technology leadership, etc.

    b. Example (small institution): Rabbi, Board Chair, two or three active and involved board members, maintenance person

2. Identify the person (or people) authorized to bring the team together during a crisis (the "crisis team manager")

    a. You may wish to designate this task to someone other than the most senior manager, as locating and bringing the crisis team together may detract from the senior manager's efforts to deal with the crisis as it unfolds

    b. You may wish to designate this task to someone other than Rabbi: he or she may be obligated to attend to religious duties

3. The crisis team manager should be able to be reached 24/7. Similarly, the crisis manager should be able to reach the members of his or her crisis team 24/7. Of course, this raises issues relating to Shabbat and holidays with work restrictions.

The function and role of the crisis team is discussed in greater detail below. But, in short, the crisis team will be responsible for restoring "command, control and communications" during a crisis while gathering as much information as possible, so that the directives of the senior manager can be well informed and effectively implemented.

In an effort to build cohesion and to work out any problems, the crisis team should practice crisis management. One way to practice this is by working through scenarios during a so-called table-top exercise, in which team members work their way through a fictitious crisis. See page 34 of the manual.

The Crisis Management Continuum: Incident Response

Incident response is the *automatic* process that an institution puts into place to ensure that employees and systems react properly to an incident as it occurs. The more standard procedures you can put into place, and on which you train your staff, the less likely you are to encounter confusion and chaos when a crisis occurs.

Such automatic processes involve careful planning, and much of the manual has been devoted to this topic.

The key point is the awareness that, during a crisis, you must recognize that the most senior manager will likely not be the one who is triggering these responses. For example, a junior staff person may find herself confronting the situation of an armed intruder or an unidentified package — and being forced to make a decision while more senior management is elsewhere. While it would be preferable if the employee could consult a senior manager about what to do during an emerging crisis, in reality, this employee may have to act immediately for the safety of the entire organization and its constituents. Your planning must be cognizant of this fact and should seek to appropriately empower such staff personnel with the knowledge of when and how to act. For examples, is your staff able to deal with the following:

1. Explosive Threats (see pages 49 – 60)
2. Armed intruders in schools (see pages 73 - 81)
3. Computer crime targeting your institution (see pages 36 - 48)
4. Evacuation procedures (see pages 56 - 58)

The Crisis Management Continuum: Crisis Management

The psychology of crisis decision making

There are a few related schools of thought about crisis management:

1. **In a crisis, a manager can do everything right — using all available information and the best possible judgment — and the decision can still make matters worse.**

This rule is perhaps most important — and the most difficult. To the extent a manager can recover from making a bad decision during a crisis, he or she has a hope of guiding the institution forward. To the extent that the manager is incapable of personally and psychologically recovering from making a bad decision, the manager will likely fail — or make things even worse than they have become.

2. **A leader will never get perfect information during a crisis situation — and leaders will succeed only where they are capable of making a decision absent perfect information.**

If a manager is incapable of making a decision under conditions of grave uncertainty or confusion, then it is unlikely that the manager will succeed in a crisis.

3. **Decisions will be reviewed by hindsight.**

It is a harsh reality that once a crisis has subsided, anyone not directly associated with the decision making process (and perhaps some who were) will begin to critically examine every decision the manager made. In some cases, as the dust settles, blame may be assigned, lawsuits may be filed, and jobs may be lost.

Managers who are daunted by this prospect may become paralyzed or take perceived "safer" decision paths that may make matters worse.

*The Moment of **Crisis***

➢ The Team

Upon the determination that a crisis has arisen, the senior manager should have her crisis manager identify those members of the crisis team that will staff this crisis and then pull that team together. In the meantime, she should focus her attention on managing the crisis.

A crisis team in action should have several features:

1. **The crisis team manager will be in charge of the crisis team absent the senior manager.** To put it bluntly: if no one is the head of the team, no decisions will be made, especially because people often resist assuming the risk of making decisions.

2. **The crisis team manager will serve as key liaison between the organizational leadership and the crisis team.**

3. **Crises are not the time for democratic decision making; they are not also the time for autocracy.** The crisis manager and the senior manager will need to hear the advice of their crisis team and make decisions in light of — but not necessarily deferring to — those recommendations.

➢ Command, Control and Communications

This is dealt with at length at several points in this manual, including at page 55. As discussed, one key role of the crisis team is to ensure that the best information available is received by management — and that the orders, decisions and communications of the organization are able to be shared with their intended audiences. This will allow management to manage the crisis as effectively as possible, and can minimize the risk that uninformed, dissident, or panicked voices will fill the vacuum.

To review some earlier discussions about command, control and communications in this manual:

1. It is essential that a decision-maker be identified, that this person have the authority to act and that the decisions can be effectively communicated to those who need to know.

a. It is important to recognize that senior managers may be unavailable during an emergency (they may be out sick or on vacation or even at lunch or away from the office for a meeting). **Thus, it is important to be able to quickly ascertain who is in charge at any given point.** Consider having a list of "succession" in the event of an absence. This will enable an institution to quickly establish a clear chain of command in light of the day's staffing and attendance.

2. Consider establishing a command center, the place where decision-makers meet during an emergency and establish command, control and communications. You may wish to have building plans, contact information and other institution-specific critical information stored at this location.

3. Have the means to communicate — and be communicated with.

   a. Know telephone numbers, fax numbers, and email addresses of key managers, constituents and media contacts. Make sure that employees know how to reach the command center to report information.

   b. Have redundant communications systems. To the extent possible, being able to reach out and be reached by more than one means may make the difference in a crisis. For instance, during a blackout or similar emergency, SMS ("texting") may work better on cell phones than cell phone calls themselves.

Besides preventing what may be counterproductive or, worse, deadly confusion during an incident, having an effective communication plan will also help you manage those outside of the immediate incident, including those who need or want information, such as the media and parents. Some thoughts, also discussed elsewhere in the manual:

1. Designate a single spokesperson for the institution. If it is necessary to have more than one, it is essential that they carefully coordinate their message.
2. This spokesperson should be the sole contact point for the media, constituents and anyone else who needs information from the institution.
3. Depending on the nature of the incident, especially if it involves children, the spokesperson might direct constituents to a further contact point.
4. Information should be clear, factual, non-emotional and consistent with law enforcement requirements.
5. The person designated to be your spokesperson should not have other, more important duties to attend to during an incident and recovery. The

spokesperson's job is to convey information. Therefore, consider how engaged in the emergency and follow-up any potential spokesperson should be.

6. The media may be interested in your incident. They may also be the most effective way to communicate important information to constituents. Depending on where you are, media may be more or less receptive to becoming a conduit for relaying information. However, if you do not wish to draw undue attention to the event, you may elect not to call the media. However, media can find out about events without your calling them — they monitor police scanners and have other sources. Thus, though you may wish to avoid media attention, it is sometimes inevitable.
7. When speaking to the media, be clear, direct and honest. Speak in short, declarative sentences. (e.g., "The facility will remain closed for the next two days.")
8. Craft your message before you are interviewed. Develop two or three key points and stick to them: e.g., "Everyone is safe, parents should call xxx-xxx-xxxx," "The institution has taken appropriate security measures," "A lawsuit has been filed." In many cases, you can answer any question with these concise, stock statements.
9. Speak to emergency officials about your message, if possible. This is especially true if a crime has been committed. The police may wish you to help them keep certain facts quiet so that they may determine if a subsequent incident is a copycat or not, and/or to ensure that an ongoing investigation is not otherwise damaged.
10. You are under no obligation to answer media questions, but note that if a story is to run, you may wish to contribute your point of view.
11. Practice.

- Impact

As you gain more knowledge, assert more command, control and communications, your ability to impact a situation should increase accordingly — to a point. As time passes, outside forces, including media, alternative voices, and other "noise" can interfere with your ability to manage and have an impact on the situation. At the same time, your ability to keep control and gather new information may degrade.

In short, the faster you can increase your ability to gain knowledge and establish command, control and communications, the more time you will have to be influential.

The Crisis Management Continuum: Business Continuity

Business continuity relates to those steps necessary to restore your institution to normal functioning after a crisis. This topic is discussed on page 101 of the manual, and is reviewed here:

Preparing for Disaster Recovery.

Disaster recovery is a critical part of post-incident work. Recovery is much easier if preparation is done beforehand.

Some thoughts on preparing for disaster recovery:

1. Maintain off-site, current backups of critical data, vendor lists, employee, constituent and donor contact lists, and other mission-critical information. This may entail someone taking a disk home with them, but if the disk or data is lost, information may get into the wrong hands. Backup security is vital.
2. Conduct an insurance review to ensure that insurance is adequate to cover all institutional needs. Keep insurance records with backup information.
3. Explore legal aspects of recovery with the institution's attorney, including discussions as to whether someone has the authority or can be designated with legal authority to take emergency steps on behalf of the institution.
4. Plan for relocating students, patients, campers, seniors, and staff ahead of time before disaster strikes.
5. Inventory everything that would cause the institution to cease operations if destroyed.
6. Review all existing service agreements and whether they include adequate post-disaster service provisions and recovery assistance.

A Word About Evidence.

There is a powerful temptation after discovering damage or graffiti to clean it up immediately. We urge you to resist that temptation and leave the entire crime scene untouched until the police arrive. By waiting, you help ensure

that valuable evidence is not lost — and that the perpetrators are caught.

It is also very useful to take photographs or videotape any evidence. Although they may not mean anything to you or even the investigating detectives, make sure to carefully take pictures of any graffiti, including any seemingly random numbers, letters or words.