ADL
Anti-Defamation League®

# PROTECTING YOUR JEWISH INSTITUTION

## Security Strategies for Today's Dangerous World




Cover Photo: Frank Ishman

Web site: **www.adl.org**

# Protecting Your Jewish Institution: Security Strategies for Today's Dangerous World

# Using This Manual

The following security awareness manual is designed to help you begin the process of thinking about security for your institution. However, it is by no means an exhaustive treatment on the subject of security — no such document exists. Moreover, it is not a security plan for your institution. Rather, it is a series of security *considerations*.

What distinguishes security considerations from a list of security recommendations? The set of facts and circumstances unique to every institution will dictate what you choose to implement. You know your institution, you know its finances and you know what security measures constituents will accept (and what leadership can help constituents learn to accept). Thus, when we offer suggestions or lists, you must evaluate those thoughts in light of your institution's needs.

**You must bear in mind that not every item on a list is applicable to your institution and that not everything applicable to your institution is on these lists.**

One way to use this manual is as a starting point for a conversation with you, selected members of your staff, lay leadership and a security professional who can assess your institution firsthand.

With all this said, we believe this manual will be helpful as you begin the process of developing a plan for your institution.

**Remember: Your ADL Regional Office is a resource available to you. To find your local ADL Regional Office and their contact information, go to www.adl.org/regions.**

ADL's National Communal Security Committee is also a resource available to you. The Committee consists of volunteers from around the country with considerable expertise in security operations, consulting, technology, risk assessment, and vulnerabilities. They can provide guidance on security issues affecting the Jewish community and are pleased to make their expertise available to the community. Those who are interested should direct specific inquiries to the ADL office that covers their region.

# Introduction: Security Planning

In order to create increasingly aware Jewish communal institutions, one must develop and utilize a security plan. A sound security plan will leave an institution better able to thwart and, if necessary, recover from, a security breach. Remember: the best way to protect your institution is to prepare for and prevent an incident's occurrence in the first place.

A sound security plan in a Jewish communal institution is often as much a management issue as it is a technical one. It involves motivating and educating all staff, leaders and community members to understand the need for security and to create and implement a coherent security plan. In general:

- Professionals and leadership should assess the risks and realities of the institution to develop a security plan, seeking professional guidance if necessary. Of course, not all institutions encounter the same risk, but all encounter *some* risk. Most critically, leaders must make sure that security is part of an institution's culture (*see* "Security in Jewish Communal Life: Building Consensus"). At the very least, input on security should be sought from all staff (not only is their "buy-in" essential for a smoothly running plan, but they are also important "eyes and ears"). When planning or participating in events, everyone—ranging from the Board President to the custodial staff — must *think security*.

- Community members have an important role in ensuring the safety of their communal institutions. Leadership can help them understand their role in the plan. Community members should:
    - Be watchful, ready, and willing to report suspicious activity;
    - Know their building — report anything out of place, missing, or that does not appear to belong;
    - Actively cooperate with security directions, check-in procedures and ticket policies;
    - Share ideas and suggestions about security and safety;
    - Help create a culture that is both secure and welcoming;
    - Support the board and professionals as they make the decision to create and implement an effective security plan.

# Creating a Security Plan

While no guide can provide a security plan perfect for every institution, there are certain basic considerations all planners must take into account. This guide will help you understand and apply those elements. ADL continually publishes new information on security and encourages you to visit **www.adl.org/security** for new materials and updates.

Creating a plan, installing hardware and/or hiring additional staff are not the end of the process. Once the plan is written, make sure that all leaders, employees and constituents know it, practice it, review it and implement it. Regular training on, and review of, your security plan are critical to your institution's security.

Creating a secure environment is a three-step process: *Assessment*, *Planning and Implementation*. **You may wish to consult with your local police and/or hire a professional security firm for assistance in this process.**

As you read through these preliminary considerations, remember that many of these topics are discussed in detail throughout this manual.

## Assessment

### Identifying Potential Threats

- What does the news tell you about the current national and international climate?
- What do police tell you about the local climate?
- What does your ADL Regional Office say about extremist and anti-Semitic activity in your area?
- What does social media tell you about the current climate?
- Is there something about your building or your staff that would attract a terrorist attack, such as high-profile programs, high-profile members or an extremely visible building?
- Are you at risk from collateral damage from an attack on a high-risk neighbor (e.g., political offices, controversial corporate offices, family planning clinics)?
- Are you at risk from employees or other "insiders"?
- Is your institution readily identifiable? The issue of signage is one to be decided by your lay and professional leadership. ADL takes no position on this issue.

### Identify Targets for Protection

Identify what you need to protect (e.g. people, property and data) and what makes those things vulnerable. There are different strategies for protecting children, adults, property and data and your planning must account for these strategies. Note also that sometimes these things are related: the theft or hack of a computer that contains membership lists, payment information, and other sensitive information can do great damage to an institution's reputation and the members' safety.

### Relationships with Law Enforcement

One of the themes ADL emphasizes in this manual is the importance of developing and maintaining a working relationship with your local law enforcement agencies. At the very least, your local police department may have a crime prevention officer who will do an on-site security inspection and review your plan. Not only could this provide useful information, but it will help build a relationship with your local law enforcement. Your local ADL office can be helpful in initiating contacts with police or other law enforcement agencies.

## Planning

### Risk Reduction

Identify the most appropriate measures to reduce your risk, recognizing that you can never completely eliminate all risk. For example, an appropriate initial step might be to replace or re-key your locks to gain control over who has access to your building or office suite.

### Command, Control, and Communications

In any emergency, firm lines of command, control, and communications are essential.

- It is vital 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 them.
- It is also important to recognize that a designated decision maker may be unavailable during an emergency (he/she 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 moment.** Consider having a "succession" list in the event of an absence, even a temporary one.

### Explosives Planning

Planning should include creating and maintaining a bomb search plan and emergency evacuation plan.

**This is an important time to contact and include your local bomb squad.**

They will help you understand what steps you are responsible for implementing in a bomb emergency (for example, searching your premises) and when they will respond, as many bomb squads will not come to a site until a suspicious item has been discovered. In fact, many bomb squads do not allow individual organizations to contact them, communicating with your bomb squad may require that your request go through the local police department. This is yet another reason to develop a relationship with your local police department. Your ADL Regional Office can help in this regard.

Your evacuation plan should include ways to notify and, if necessary, evacuate everyone in your facility in an emergency. Designate a meeting point to ensure that everyone is safe.

- You should create plans that deal with the varied uses of your buildings. School days, high traffic events (such as the High Holidays) and days when the facility is not used all create different security circumstances.

### Business Recovery

Planning should include business recovery strategy and a review of insurance. Such business recovery plans may include off-site data storage (including vendor, membership lists, and other sensitive information) and plans for emergency corporate governance, etc.

### Available Resources

Work with security specialists, the police, other emergency services as well as your Anti-Defamation League Regional Office.

## Implementation of a Plan

### Accountability: The Security Manager

Designate a member of your staff as security manager who would be accountable for implementing, reviewing, and regularly updating the plan. Make sure everyone is trained to implement the plan — especially those who will be on the front lines of using the plan and those who know your building best: your maintenance personnel.

The security manager should be a member of the senior staff, yet he/she should have enough time to fulfill his/her security responsibilities, especially when first assuming the position (for, if as in most institutions, the security manager has no security experience and thus may have a significant learning curve to overcome). This person will also be responsible for continued training and for updating the plan.

### Training Is Critical

Conducting communal and staff training, drills and role-playing and regular refresher exercises is critical. Drills and role-playing ensure that the plan is workable, up-to-date, fresh in people's minds, and will develop sound security instincts. Security is a continuous process.

### Implementing the Security Plan

You and your security team must regularly assess your plan based on world, national and local events.

### Build Relationships

At every stage, work to build relationships with your local emergency services as well as your neighbors. Get to know local law enforcement and get them to know you *before* there is a problem. Invite local police officers to use your gym, to join you for an *oneg shabbat* or just to visit your building and get to know it.

### Review and Revision

Security requires constant reassessment and updating. An outdated plan can, in many instances, be worse than no plan at all. We suggest that you establish a timetable for reviewing and revising your plan. Moreover, we suggest that you establish a training program that will help keep security skills fresh. (Please see section on Security Training.)

## Security Committees

Your organization may benefit from the creation of a security committee. A security committee can help bring staff and leadership together to ensure that there is maximum "buy-in" to a security plan. Depending on the type of institution, professionals and leadership working together can help ensure that the institution's wider constituency accepts the plan and thus complies more readily with implemented changes — something that can mean the difference between effective solutions and failure. Moreover, leadership can work to reassure constituents, without revealing too much, that the institution takes security seriously. Security planning is a process that may be undertaken by a security committee with the advice and consent of your board.

### Small and Mid-Size Institutions

This manual is intended for institutions and budgets of all sizes. Remember: many of the suggestions included in this manual are no-cost or relatively low-cost ideas (e.g., using ushers, re-keying locks for key control, etc.).

### Security 'Philosophy'

Security is a long-term issue. It is not something that one can effectively address every time there is a new alert or increased sense of risk. Solutions hastily implemented under such circumstances can be costly and less effective than solutions implemented as the result of careful planning. In other words, security is something to be addressed rationally and in a considered fashion, not reactively and out of fear.

**Please remember, a security expert can help you fully examine these issues, and create a plan to implement.**

## Planning Snapshot

Security is a long-term process. No one plan works for everyone. However, depending on what is best for your institution, you may wish to consider the following. Remember, these topics are discussed in detail later in this manual.

**Establish access control systems. Ensure that entrances to your building are monitored; no one should enter your building unscreened.** There are many ways to screen, including using ushers, volunteers, staff, etc. The installation of closed-circuit TV cameras, intercoms and door release systems can assist in this process. Your security plan should develop and implement policies to ensure that screening is ongoing.

**Minimize the number of open entrances to your facility (consistent with fire codes).** A culture that promotes security consciousness allows staff and visitors to understand that minor inconveniences may translate into major security benefits.

**Have all emergency phone numbers readily available.** While you should always try to use 911 first in any emergency, you should also have the phone number of your local emergency responders readily available. Have cell phones available to call emergency services from outside your facility

**Note:** *Do not use a cell phone or walkie-talkies during a bomb-related emergency as any instrument using radio waves may cause a device to detonate*

**Use available resources to document suspicious behavior.** Using smartphones or tablets or other devices, take pictures or videos (when it is safe to do so) that may assist police if a suspicious individual or car is seen.

**Regularly inspect your building.** You should be able to quickly ascertain if something is amiss and help law enforcement if there is a problem.

**Utilize security devices you already have.** Ensure that security devices are turned on and functioning, that outdoor lighting is working, that windows and fence lines are kept clear of bushes and that access to your building is appropriately limited and consistent with fire codes.

**Think security.** Each person is a "deputy" in the effort to maintain proper security. Good security practice flows down from top management. It is important administrators share security information with their staffs and with lay persons to increase the security consciousness of the entire organization. Security awareness should be built on a broad base which begins at home, continues on to the street and public transportation and culminates with sound security planning and practices in the employees' work areas. The key point is to recognize unusual activity.

# Physical Security and Operations

## Important Note

While the suggestions offered in this chapter can be quite detailed, it is important to recognize that no manual can anticipate the unique circumstances at any institution. Therefore, use the suggestions given below as starting points for discussions with a security professional who will be able to assess your institution's particular set of circumstances and make specific recommendations.[1]

Physical security starts with a rather simple basic premise: those who do not belong on your institution's property should be excluded from your institution. This may happen in three (often interrelated) ways:

1. When those who do not belong are identified, stopped and denied admission by a person.

2. When those who do not belong are denied admission by a physical device, such as a locked door.

3. When those who do not belong are denied admission because they decide that your institution is too difficult to enter and thus they do not even try.

This section will consider the various methods of excluding those who do not belong:
- Access Control
- Key Control and Locks
- Protective Devices and Alarms
- Windows and Doors
- Fencing and Gates
- Protective Lighting
- General Deterrence

[1] Given the specific information discussed in this chapter, it is important to again specifically mention that neither this guide nor this chapter is intended to provide comprehensive, institution-specific advice on security matters nor is it meant to replace the advice of a security professional. For comprehensive, institution-specific security advice, a security professional should be consulted. ADL specifically disclaims any and all responsibility for, and is not responsible for, any loss or damage arising out of use, nonuse or misuse of this information.

# Access Control

Access control means that, when your facility is open, no visitor, delivery service person or unknown individual is able to enter your facility without being both *observed* (directly or indirectly) and *approved*. Several techniques to accomplish that goal may include any or all of the following.

## Security Desk

A security desk should be set up in the main lobby of each building which has an open-access or open-door policy. A sign-in/-out log, supervised by an employee who validates identification *prior* to allowing visitors to proceed into the building, is highly advisable.

## Monitored Entrances

Ideally, an institution should have a single entrance only, monitored by a staff person and equipped with an intercom system for communicating with anyone who comes to the door. Simply, an open door policy does not mean that every door need be left open and unlocked.

## Checking Credentials

Before allowing a person to enter institution property, seek to make certain his/her identification papers or other credentials (including membership cards) are valid. Police and most utility employees carry identification cards and other documents. It is critical to remember that your employees can probably not tell the difference between valid and forged documentation or credentials. It is questionable whether your staff can be expected to tell the difference between the real and the fake. It is very easy to purchase a uniform or equipment that enables an intruder to pretend as if he/she has legitimate reason to enter your facility, and without verifying a person's identity or legitimacy, it will be difficult to identify a potential intruder. It is worth a few moments to contact the person's company or organization to determine the legitimacy.

**NEVER BE EMBARRASSED TO ASK FOR MORE IDENTIFICATION OR TO ASK A PERSON TO WAIT UNTIL HIS/HER IDENTITY MAY BE CHECKED. ANY INDIVIDUAL WHO BECOMES AGITATED OR ANGRY AT SUCH A REQUEST SHOULD BE CONSIDERED OF QUESTIONABLE LEGITIMACY.**

## Visitors

At no time should visitors be allowed to roam freely through your property unescorted or without being observed. That is especially true for individuals who expect to work on your most sensitive systems such as burglar alarms, fire alarms, communication systems or computers. Special diligence should be applied to those individuals when they visit your institution even if they are legitimate. For larger institutions, certain areas should be considered off-limits to all but authorized personnel.

**Note:** Some institutions specialize in open and free access, e.g., facilities with gymnasiums. Allowing visitors free access to your facility does not mean that they should be allowed to go anywhere (e.g., into restricted areas such as office spaces) or that they should be given a sense that their actions are entirely unnoticed by the institution's personnel.

## Stay-behinds

End-of-day locking procedures should include a visual examination of all areas to prevent "stay-behind" intruders.

## Photo Identification:
## Employee Photo Identification Cards and Badges

All employees should have and wear identification. Such badges make identification of non-employees immediate. Moreover, such cards will not only enable visitors to immediately identify those who work in an institution but will psychologically help employees understand that they are part of their agency's security team. Photo identification should only be provided with accompanying education regarding their care, the procedure to be followed if they are lost, as well as the manner in which employees should approach unknown individuals.

Creating ID badges requires thought. Cards should have clear pictures along with the employee's name. The institution's name should not necessarily be placed on the card. In any event, employees should be instructed that their card should be prominently worn while in the building and, for their own safety, kept from view when away from the building. There is no reason why a person in the street or in a train should be able to identify who you are and where you work. Lost cards should be reported immediately.

# Key Control and Locks

## Key Control

Knowing who has which keys to which locks at all times is a vitally important issue. Failure to maintain such control may defeat the entire purpose of creating a security system. Institutions often simply assume that no one leaving their service — either an employee or volunteer — will subsequently break into their building or office. A sound key-control policy is essential to an effective security program. There should be a central key control location where masters are kept and access to which is strictly controlled.

### Other Thoughts

**Registry.** A central key control registry should be established for all keys and combinations. Employees and leadership should be required to sign for keys when they are received and the return of keys should be an important part of an exit process.

**Issuance.** Supervisory approval should be required for the issuance of all keys and locks. Spare keys and locks should be kept in a centrally located cabinet, locked under the supervision of a designated employee. Master keys should be issued to a very restricted number of employees and these should be inventoried at least twice each year.

**Re-keying.** When key control is lost, it may be worthwhile to have an institution's locks re-keyed.

**Combination Locks and Codes.** Where combination locks and coded locks are used, those combinations and codes should be changed at least every six months or when employees or leadership leave your employ. Combinations should also be kept under strict control of management.

**Special Keys.** It is good policy to use locks with keys that cannot be duplicated on the outside without a special key.

**Key Card Readers.** Key card readers, while expensive, make key control and locking more effective. You should designate who receives what form of access, i.e. time/day/weekend etc.

.

## Locks

Locks are, of course, particularly important to security. **We encourage you to consult a professional locksmith.** While the suggestions offered in this section are especially detailed, it is important to recognize that no manual can anticipate the unique circumstances at any institution. Therefore, use the ideas addressed below as starting points for discussions with a professional locksmith who will be able to assess your institution's particular set of circumstances and make specific recommendations.

Door locks should be chosen and installed to provide proper security for the location involved. Locks with single cylinders and interior thumb turns, installed on doors with glass panels, should be placed more than 36 inches away from the nearest glass panel. Dead bolt locks are the most reliable and should seat at least an inch into the door frame or lock-bolt receiver. Padlocks should be of high-grade material designed to withstand abuse and tampering.

**AT ALL TIMES, THE DOOR-LOCKING SYSTEM MUST MEET THE FIRE CODE TO ALLOW EMERGENCY EXITING WITHOUT IMPEDIMENT .**

**Exterior Locks.** All exterior door lock cylinders should be protected with metal guard plates or armored rings to prevent cylinder removal. The guard plates should be secured with round-head carriage bolts. Some highly pick-resistant cylinders have a guard plate assembly built around them.

All exterior locks should conform to the following.

- Lock cylinders should be highly pick-resistant.
- Where possible, dead bolt locks should have a minimum bolt extension of one full inch.
- Drop-bolt locks should be installed with the proper strike: wood frame, angle strike; metal frame, flat strike.
- Metal guard places or armored rings to prevent cylinder removal. The guard-plate should be secured with round head carriage bolts. Some highly pick-resistant cylinders have a guard plate assembly built around them.
- The jamb must also be sufficiently strong. A strong lock entering a weak jamb will fail in its purpose.
- At all times, the door-locking system must meet the fire code to allow emergency exiting without impediment.

**Automatic Closers.** Doors that have air, hydraulic or spring returns should be periodically tested to ensure that doors consistently return to their fully closed or locked position.

**Lock Management.** Your institution's security manager should be responsible for the following:

- ✓ Regularly inspecting and reporting all defective and damaged locks; repair quickly
- ✓ Establish a chain of responsibility for all locks (doors, windows, etc.); ensure locks which are to be locked are in fact locked and report all failures to do so.
- ✓ See that keys are not left unattended
- ✓ Recommend installation of additional locks if necessary

**Remember: locks are present not only on doors, but on windows, offices, filing cabinets and storage closets as well.**

## Protective Devices and Alarms

**This is an area where professional advice is particularly needed.** Begin by contacting your local law enforcement agency and request help from the crime prevention, crime resistance or burglary prevention officers who are specially trained and can offer expert guidance. Keep in mind that an officer is not selling a product or system but is there to help you.

### Protective Devices

Protective devices — intrusion detectors, fire detection, alarm systems and cameras slaved to a closed-circuit TV (CCTV) system — can be an important (and sometimes costly) part of an institution's security system. CCTV coverage may also be useful as such systems permit surveillance of exterior exits and interior halls by one trained security officer at a master console. However, even the most sophisticated and costly devices are limited by the human factors involved. The best CCTV system will be ineffective if it is not properly monitored or if those tasked with monitoring the cameras are overworked, poorly trained, tired or distracted. Additionally, most institutions are unlikely to have the resources for continual monitoring. Most systems now include video storage systems, but here, too, the best video surveillance system will fail when not properly used, e.g., when no one is assigned the job of checking, reviewing and deleting un-needed stored videos.

## Other Thoughts

- Surveillance cameras should be conspicuously placed at the entrance points to your institution to act as a deterrent to potential intruders. Cameras may also document criminal acts that may occur on your property. This documentation can be used to identify and prosecute perpetrators. Although expensive to purchase initially, these cameras generally prove to be economical when compared to potential loss.

- Use a wide-angle lens to survey entrances.

- Consider using cameras that employ infrared illumination to enhance nighttime video or provide adequate lighting.

- Couple the camera with a time-lapse recorder for permanent recording.

- Make sure your camera has a time/date recording capability, and it is working. Compare the cost of color versus black and white.

- Save video film for a minimum of 72 hours, permanently if anything of a suspicious nature is seen.

- Check for updates security system software on a regular basis.

## Alarms

This is another area where professional guidance is strongly recommended. Alarm systems are designed to protect your institution from intrusion. The installation of an alarm system can materially improve the security of most institutions. The sophistication and coverage provided vary widely from system to system.[2]

The size, location and type of institution will help determine the type of system required.

[2] Most alarm systems are made up of three components: (1) a sensor, which detects an intruder, (2) a control, which receives information from the sensor and (3) an enunciator, visibly, audibly, or electronically alerting someone of the intrusion

Motion detectors or automatic sensors that respond to sound or movement are excellent protective devices used alone or in conjunction with your institution's lighting system. These detectors and sensors are economical and they can be used inside or outside of your setting.

Because there are many alarm systems on the market, you should research each system and select the one that best suits your needs.

Whatever the amount of money you choose to invest in a dependable alarm system, it is generally less than the amount of damage that might be caused to your institution by an intruder gaining access.

When installing an alarm system, consider the following.

- Make sure all alarm systems have emergency backup power sources.
- Conceal the alarm control box, lock it, and limit access to it.
- Every system should have an electronic circuit delay of at least 30 seconds.
- Ensure that the alarm can be heard throughout the property and have the alarm system monitored by a central alarm monitoring company.
- Make sure all wiring components and sirens are protected from tampering.
- Make sure the alarm comes with a "test" option. Testing the system regularly is a vital component of maintaining the effectiveness of your alarm.
- Check with your insurance company regarding their requirements and suggestions for alarm system configuration.
- Investigate a cell phone based auto-dial/alert option for your alarm system.

## Windows and Doors

### Windows

Windows should provide light, ventilation and visibility, but not easy access. Glass bricks can be used to seal a window, allowing a continued light source while providing increased security, although visibility and ventilation will be diminished. Gates and expanded steel screening, while often unattractive, will provide a high degree of security. Local building

codes and fire safety regulations should be consulted prior to all such installations to avoid costly violations. Also, note that sky-lights, ventilators and large door transoms can provide easy access to intruders unless properly protected. If permanent sealing is not possible, steel bars or screens of expanded metal may be required (if permitted by fire codes).

## A Critical Note on Glass

Flying glass can be as dangerous in an explosion as the actual explosion itself. Consider replacing traditional glass with safety or shatter-resistant glass or using a clear protective film to secure the glass to the frame.

## Doors

All external doors, main building doors, and lobby doors leading to common halls should conform to the following guidelines.

- Solid core, wood or metal.
- Glass door panels or side panels should be reinforced either with metal or some form of steel mesh. Barring that, they should be replaced with a glass that does not shatter easily.
- Where there is an alarm system, "glass breaker" sensors that detect glass breakage should be installed close to glass doors or windows.
- Door frames should be sturdy and appropriate for the type of door. Weak frames should be replaced or rebuilt.
- Exterior door locks should conform to the guidelines found in the section on locks.
- Interior or office doors should be equipped with heavy-duty, mortised latch sets that have dead bolt capability. Rim-mounted, dead bolt or drop-bolt locks can be installed to increase security of important offices or rooms.
- Doors that have external or exposed hinges may be vulnerable to pin removal. The hinge pin should be made unremovable by spot welding or other means or the hinges should be pinned to prevent separation.
- Doors to utility closets should be equipped with dead bolts and kept locked at all times. Such closets, if unsecured, can become hiding places for "stay-behind" criminals or for the placement of explosive devices.
- All exterior doors which do not have glass vision panels should be equipped with wide-angle viewers (peepholes).

- Interior doors should have two-way visibility at stairways, corridors, etc. There should be a clear view of room interiors from the doorway. Note, however, lockdown procedures (see section on lockdown procedures) may require the use of rooms without windows, or, at least, doors whose windows can easily be covered.
- Access to offices, kitchens, electrical and mechanical rooms and storage rooms should be limited to appropriate staff and be locked when not in use.
- Fire doors must conform to all local fire and building codes and should have an underwriter's laboratory rating.
- Fire doors should be secured with approved latching or locking hardware, such as a panic bar with a spring latch or safety lock.
- If a fire door has a solid core, the interior material must be fire resistant.
- An adjustable spring or air return will ensure that the door is always closed.
- Consider the possibility of placing height marks next to exit doors to help employees estimate the height of suspicious persons.
- As with all doors, sensor devices connecting to a sound device or system will announce their opening.
- All doors or gates not observed either directly or remotely should be kept secured.
- Staff should be discouraged from using wedges to keep outside doors open.

## Fencing

Fences make an intruder's entry more difficult and give the appearance of a more secure institution. The following thoughts need to be prefaced with an important warning applicable to all sections of this manual: take note of all local building and zoning codes regarding fences and walls prior to planning or contracting.

Some thoughts to bear in mind:

- Consider open ornamental fences — in preference to walls — as they do not block visibility, are less susceptible to graffiti and may be more difficult to climb.
- Fences should be at least six feet high. Therefore, an institution should take advantage of any small incline or hillock along which to build the fencing.

- Fences should also be designed so that a person cannot reach in with his/her hand or a wire to open the fence gate from the outside.
- If a panic bar is required on the inside of a fence gate, a solid metal or plastic shield should be used to prevent a person on the outside from opening the gate.
- It is important that whatever physical barrier one erects should be in concert with the aesthetics of the neighborhood or environment.
- **It is unwise to alienate neighbors who may serve as part of a neighborhood watch and provide additional "eyes and ears" as part of your overall security program.**
- Walls should be constructed where there is a need for privacy and/or noise control.
- Fence lines should be kept free of trash and debris. Clear away trees and vines that might aid a climber. Weeds and shrubs along fence lines, sides of buildings, or near entrance points could hide criminal activities. Keep shrubs low or clear them away completely. Cut back vines attached to buildings in order to prevent determined intruders from gaining access to upper windows or unprotected roof doors.

**Note:** No barrier is foolproof. It is impossible to erect an impenetrable physical barrier that is unprotected by personnel. Even when protected by personnel, human beings grow fatigued, inattentive, bored or simply make mistakes.

## Protective Lighting

The value of adequate lighting as a deterrent to crime cannot be overemphasized. Adequate lighting is a cost-effective line of defense in preventing crime.

### Some Considerations on Lighting

- Lighting, both inside and outside, is most helpful and can be installed without becoming overly intrusive to neighbors.
- All entrances should be well lit. Fences should also be illuminated.
- For outside lighting, the rule of thumb is to create light equal to that of full daylight.

- The light should be directed downward away from the building or area to be protected and away from any security personnel you might have patrolling the facility.
- Where fencing is used, the lighting should be inside and above the fencing to illuminate as much of the fence as possible.
- Lighting should be placed to reduce contrast between shadows and illuminated areas. It should be uniform on walkways, entrances, exits, and especially in parking areas.
- Perimeter lights should be installed so the cones of illumination overlap, eliminating areas of total darkness if any one light malfunctions.
- Fixtures should be vandal-resistant. It is vital that repair of defects and replacement of worn-out bulbs be immediate. In addition, prevent trees or bushes from blocking lighting fixtures.
- You may wish to use timers and/or automatic photoelectric cells. Such devices provide protection against human error and ensure operation during inclement weather or when the building is unoccupied.

A security professional should be contacted to help you with decisions on location and the best type of lighting for your individual institution.

## General Target Hardening

One function of security devices, lighting, fences, etc., is to make your facility look less inviting to a potential intruder. The more uninviting your institution is to such an individual, the less likely the incursion. This is called "target hardening." While an institution should not reveal the details of its security measures, providing a potential attacker with clear evidence that a security system is in place will often deter an attack before it happens. Some examples of deterrents:

- Signs indicating the presence of an alarm system.
- Visible security foot and/or vehicle patrols.
- Well-maintained fence lines and lighting.
- A general appearance of a well-maintained facility.
- Regular presence of local law enforcement on or near your grounds.

# Relationships with Emergency Personnel

It cannot be overemphasized that developing relationships with your local emergency responders will enhance the security of your institution. We believe that this is a critical component of any effective security program.

The following are some suggestions on how to build relationships with your local emergency responders. In many cases, your ADL Regional Office can help facilitate these relationships.

## Law Enforcement

Have a meeting with the local police commander (precinct captain, substation commander, etc.). He/she will be more than happy to meet with you. The meeting should include the local commander and the lieutenant or sergeant responsible for patrol officers in your area. Ascertain what information they need from you so that they may more effectively provide service. This is important because *all* these officials have limited resources and you need to demonstrate that you are not only asking for assistance, but that you are supportive of their efforts and are an active participant in your own security.

- Meet the patrol officers who will be the first responders to any call from your institution. This may take three meetings — including one night meeting — given changing shifts. You should seek to develop a personal relationship and an understanding on the part of officers of the role your institution plays in the community as well as your concerns.
- You may wish to offer your facility as a place for officers to use the restroom, have coffee or even as a quiet place to write reports.
- During special events (including holidays), you should keep your local police department informed as to the times and the nature of your event. It is also useful to advise them of times when people are typically walking or driving to and from your institution.
- Most larger police departments have crime prevention officers. As we have said elsewhere, seek their advice on your security plan and ask about any security issues they may observe.

**Note:** although this is changing in light of September 11, crime prevention officers are typically concerned with issues of burglary, theft and the security of your institution from those who seek pecuniary gain. While there is a great overlap between an anti-crime audit and a security audit, they are not synonymous. For example:

- If your local department has a special weapons and tactics team (SWAT), consider having a SWAT officer map your institution and its property and determine what information would be helpful in the unlikely event that a SWAT team is called to your institution.
- It would also be useful to have a member of the bomb squad talk to your appropriate staff. This would also be a good opportunity to consult with the bomb squad regarding the information they need from you to be effective. You may need to go through your local police department in order to have access to a bomb squad.
- If appropriate, consider volunteering your site to serve as a location for SWAT or bomb squad training.
- Note that officers' assignments tend to change with a degree of regularity; meeting once will not ensure that you have a relationship with the appropriate person. In short, unless you meet the new people, they will not know who you are.

## Fire Department

Meet with local fire officials, such as the commander of your fire station, the department, or a member of the fire marshal's staff. It may also be useful to meet with a member of the local arson squad. As with the police department, recognize that these officials are under budgetary and time constraints, though they should be willing to have someone review your facility and its fire plans.

It is also advisable to meet with local EMT personnel to help create a medical emergency plan. Things to consider:

- First aid and CPR training for staff.
- An emergency medical kit or kits appropriate for your institution (including the acquisition of an automatic defibrillator machine).

In all cases, recognize the extraordinary service all of these individuals provide our communities. Working with them will enhance their ability to serve your needs.

Finally, it is worth having and sharing plans of your facility with local emergency responders. If they are unwilling or unable to keep them on file, consider having them stored in a secure nearby, off-site location for quick access during an emergency. Check with emergency responders to determine which information they will need and where they believe the data should be safely stored. Have a "go to" plan ready that can provide them with the information they may need, such as a floor plan and information on where important assets are located.

# Security in Jewish Communal Life:
## Building Consensus, Training and Preparedness

In one very important sense, security decisions are no different from other tough decisions you make and implement. Such decisions require the same kind of organization, leadership, assessment of priorities, etc. that might be required by a capital campaign, for example. *As we know from our experience elsewhere in Jewish communal life, change requires leadership and leadership requires both hearing many voices and making tough decisions.*

## Building Consensus

In order to prevent resistance to or misunderstanding of security measures taken or not taken by your institution, such decisions must include input from management, lay leadership, staff and other constituents. Information-sharing and participation are vital components to building consensus.

When people understand the justification behind increased security measures, they are more likely to be supportive, active participants and, perhaps most importantly, less fearful. As we have said elsewhere, such support and participation from the members of your institution is critical to the success of a security initiative.

### Managing Different Views on Security

In keeping with the open nature of the Jewish community, all voices should be heard and given appropriate consideration and respect.

We believe that the overwhelming majority of parents, congregants and other constituents already understand the need for increased security and are seeking reassurance from leadership as well as an opportunity to be an active participant in the decision-making process. We also understand that people can be resistant to the additional restrictions or costs imposed by new security procedures.

Again, steps to creating a security consensus should be familiar to anyone in organized Jewish communal life. The process is no different from any major decision-making process that occurs in your agency.

These steps include:

**Needs Assessment.** The best antidote to reticence and fear is being able to present your case calmly, rationally — but with sympathy for your interlocutor. You may wish to (and your ADL Regional Office can help):

**Develop a case for security in your area.** Security is an international, national and local concern. Your institution requires protection from a variety of potential threats. No area is immune and no Jewish institution can be viewed as so small or so remote that it does not require thoughtful security measures. ADL's experience with anti-Semitic incidents nationwide underscores this important point.

**Conduct security seminars and programs at your board and constituent meetings.** By bringing in knowledgeable speakers and by circulating this information book, you can demonstrate that security is neither complicated nor necessarily prohibitively expensive. These activities will lay the groundwork for initiating a dialogue about your institution's security plans. Point to other institutions that have already initiated security programs to create an environment of leadership by example.

**Buy-in.** An effective security response for your institution requires "buy-in" by the constituents of your institution, including professional staff and lay leadership, especially those who can make decisions that impact the institution and can allocate or raise necessary funds. Moreover, when presenting the case for a security program to either a board or constituents (e.g. parents), it is important that you be candid about the necessity for upgrades to institutional security. Do not, however create an atmosphere of fear and anxiety.

We believe that this process should be:

- Conducted in an environment free from exaggeration and hyperbole. Indeed, this process must scrupulously adhere to the principle that a calm, rational decision-making process is an essential ingredient to success.
- Honest and candid.
- Open to ongoing input from all agency stakeholders.
- Participatory to both analyzing the needs of your institution as well as to the decision-making process designed to address those needs.
- Inclusive of relevant community institutions (e.g., law enforcement).

Your ADL Regional Office is available to you as a resource during this process.

**Note:** In order to generate support for a security program, one might be tempted to overstate the security risks confronting one's institution. There are many reasons why producing a fearful environment is not a good strategy: It will alienate people from the institution, lead to poor decision-making, may result in the allocation of funds away from simple and effective security steps and it lessens the speaker's credibility at a time when credibility is critical. It is also unethical to generate additional fear to accomplish a goal.

## Dealing with Disagreements

In institutions where senior management and/or leadership are hostile to the idea of examining their security procedures, it is worth speaking to colleagues and like-minded constituents or lay leaders. They may be able to help develop a consensus.

## Ongoing Consensus

As noted elsewhere, we recommend creating a security committee. A carefully selected security committee will assist you in identifying potential security problems and developing possible responses. Moreover, such a committee will help analyze recommendations, concerns and suggestions from your constituents. The committee should have responsibility for the development of ongoing security procedures and training.

Amongst others, the committee might include the following participants.

**Board members.** Members of the board may provide knowledgeable and energetic support — and serve as allies for change and possible expenditures.

**Trained constituents.** Members or supporters of your institution may include individuals with police, security or emergency medical training.

**Parents.** Understandably, parents are concerned about the security of their children; their voices must be heard. Consider the creation of an official parent liaison to the security committee.

# Training and Preparedness

Security professionals understand that security skills — including knowledge of procedures, alertness, and attention to detail and change — degrade over time. This diminution of skill may occur quite rapidly. Moreover, without constant testing and evaluation, security plans quickly become stale and out-of-date. To remain effective, any security plan must include regular training, evaluation and testing.

Ongoing training has another advantage: it reinforces the vitally important message to your staff and constituents alike that management remains dedicated to the long-term safety of those who work in or utilize your facilities.

We understand and are sympathetic to the demands on time and energy faced each day by professionals in the Jewish world. Full schedules and limited resources make it difficult to add another routine to the week. However, we believe that many of the activities described below can take less than 30 minutes a week on average and will yield a significant benefit to your institution.

## Training Management

As this manual has repeatedly noted, every member of an institution is responsible for security on some level. While some employees have more direct responsibility than others (e.g., security officers, door personnel), everyone requires training and refresher information. This chapter will not deal with the training of those who are full-time security personnel; security officers, security managers, and door personnel require constant, ongoing training and should practice their skills at least weekly.

For the remainder of your employees, institution leaders may wish to adopt the following training schedule.

### Yearly and/or Semi-Annual Major Drills

Once a year — more frequently if necessary — the staff should spend some time participating in a security discussion and/or drill. Topics might include:

- Evacuation (similar to a fire drill)
- Phone threats
- Bomb searching techniques
- Security procedures review
- Lockdown procedures (in schools, etc.)

Drills might be conducted in conjunction with local emergency management personnel.

## Monthly Courses, Seminars, Role-Playing Sessions

Each month — perhaps at a monthly staff meeting — you should engage staff members in shorter (10 minutes or so), information sharing, policy discussion, and role-playing sessions.

Topics, depending upon your institution's needs, may include:

- Access to areas with children and pick-up procedures
- Closing procedures
- Computer access
- Dealing with vagrants
- Handling phone threats
- Information security
- Key and lock security
- Lock-down procedures
- Making an effective 911 call
- Procedures for dealing with bomb threats
- Procedures for reporting security violations
- Visitors/visitor restrictions

## Weekly Security Refresher Discussions, Notices, Reminders

Posters, discussions at weekly meetings, e-mailed security "tips of the week," etc., are all methods of achieving ongoing training and may help keep skills sharp. One innovative idea is to e-mail short scenarios to staff. Explain the purpose of these scenarios beforehand to avoid unnecessary anxiety among staff. For instance:

- "If stairwell C were closed off, how would you evacuate the building right now?"
- "If you received a bomb threat by e-mail, what would you do right away?"
- "A man in a phone company uniform and a valid-appearing photo ID badge comes to your desk asking for access to your phone and computer; what do you do?"
- "You look out a window and see a person taking photographs of the institution; what do you do?"

While employees need not respond to the message, it is an opportunity to think through responses. These scenarios might also be presented for discussion at staff meetings.

## Training Methodology

While security training is often designed in a lecture format, information retention will be improved by involving staff in the learning process. Consider using role-playing scenarios, "best" and "worst" practices and case studies when discussing security with staff and constituents. Even 10 minutes of role-playing or discussion of a scenario will be more likely to sharpen your staff's security skills than a lecture on the same topic.

Management should also encourage staff and community recommendations for procedural and physical security improvements. Helpful suggestions can then be acknowledged at both staff and board meetings, which will create an atmosphere where taking an interest in security is acknowledged.

## Security Committees (See previous section dealing in Security Committees.)

As discussed elsewhere, a security committee can assist you in maintaining a high level of awareness and training. The committee should have responsibility for ongoing maintenance of security procedures and training and can help devise and implement your training regimen. A security committee provides an excellent opportunity for involving lay leaders in the security of your institution.

# GUIDE TO DETECTING SURVEILLANCE OF JEWISH INSTITUTIONS

Jewish institutions are often called upon to "be alert" for suspicious activity. This brief guide is designed to help you do that.

- Keep your eyes and ears open for anything unusual or suspicious and call law enforcement immediately if you come across something. **Trust your instincts.** If something strikes you as being out of place or problematic, call the police immediately.
- Unusual behavior, suspicious packages and strange devices should be promptly reported to the police or security personnel.
- Requests for information, particularly about security or procedures for your building, should also be promptly reported.

**Report surveillance immediately:** Watch for people who[3]:

- Record data about your institutions by sketching, note taking, videotaping, or taking pictures.
- Sit in a vehicle for an extended period of time, including after regular business hours.
- Loiter near your facility or in the lobby of your facility.
- Arrive at your facility without prior notification (may claim to be contractors or service technicians, etc.).
- Attempt to deliver packages or other items to an office or to a specific person.
- Attempts to by-pass your security, even "accidentally" walking past a check in desk.
- Appear to be measuring distances in stride.
- Are uncooperative, dismissive or pretend not to understand what you are talking about if challenged by a representative of your institution.

Surveillance may include an attempt to **"probe"** your security, for example:

- An attempt to remove property from an office or a facility without proper authorization.
- Leaving unattended packages in or around facilities to see how they are dealt with.
- Acting uncooperatively, dismissively or pretending not to understand what you are talking about if challenged by a representative of your institution.

---

[3] of course, many of these activities are perfectly consistent with innocent behavior. Adopted in part from http://www.homelandsecurity.state.pa.us/homelandsecurity/cwp/view.asp?A=3&Q=148830

- Attempts to by-pass your security, even "accidentally" walking past a check in desk.

**Pay attention to details.** What seems unimportant to you may prove to be important to law enforcement.

**There is a natural temptation to explain away inappropriate behavior and not report it.** Resist that temptation, and feel comfortable in approaching law enforcement to explain why you are suspicious. Even if you think you might be wrong, remember that it is law enforcement's job to filter out good information from bad. At the same time, institutions should ensure that all staff members and constituents feel comfortable reporting suspicious activities to their superiors.

**Report even minor concerns.** You do not know what else has been reported and whether your "small" detail fits into a larger puzzle. If you see suspicious behavior, do not confront the individuals involved.

Consistent with your personal safety and institution's policy, take a picture and/or take a note of the details using the SALUTE method:

**S** - Size (Jot down the number of people, gender, ages, and physical descriptions)

**A** - Activity (Describe exactly what they are doing)

**L** - Location (Provide exact location)

**U** - Uniform (Describe what they are wearing, including shoes)

**T** - Time (Provide date, time, and duration of activity)

**E** - Equipment (Describe vehicle, make, color etc., license plate, camera, etc.)

Ensure that your institution's rules and procedures dealing with who gets into your facility are sufficient and are being implemented ("access control"). More generally:

- Ensure that security devices that you have are working and are used. This includes ensuring that your outdoor lights are working and used as designed, your door and window locks are functioning and locked, your alarm system is functioning and turned on, and that any precautions you use to secure your computer systems are in place and up-to-date.

- Ensure that your staff knows what to do in the event of an emergency.

- Practice your security procedures, reviewing with all personnel their role in security. For instance, if vigilance has slipped in mail and package delivery safety procedures, now is the time to revisit this area.

- If you have not done so, this is an excellent opportunity to invite your local law enforcement to your institution to discuss security. ADL can help you make these contacts if you do not already have them.

We also strongly recommend that you consult the guidelines and advisory materials on the ADL web site at www.adl.org/security/ .

**Security awareness needs to be part of your culture each and every day in order to be effective.** If you have not established security policies and procedures for your institution – including providing all staff with behavioral profile training – please contact the ADL office so that we can assist you in making sure that your institution remains safe for all who enter it.

# Computer and Data Security

Computer and data security should be an integral component of your security program. An unsecured system may leave members, donors and staff open to personal harassment and financial difficulties and be an embarrassment for your institution. Your institution can be crippled by a computer attack before you even know what has happened.

In this chapter we will explain how your computer system may be vulnerable to attack, either by outsiders illegally accessing your IT infrastructure or by malicious insiders. Though nominally geared toward those with small networks (representing many if not most of our institutions), this information is critical for even those agencies using one computer with no connection to the Internet.

We will also look at specific aspects of IT security and recommend procedures to ensure your network is secure.

In the final section of this chapter, we will discuss the use of the Internet, particularly the risk institutions face when posting certain types of information on their Web sites.

**Due to the complexities of these issues, ADL recommends you consult a computer security professional for the most comprehensive security plan.**

The key to your institution's data security depends on how that data is stored. Most institutions have either a stand-alone computer which connects to the Internet via high-speed connection, wireless, or tethered to phones and other mobile data devices or they have a network that connects to the Internet using similar methods as mentioned above.

If your computer or network is connected to the Internet by a high-speed connection, wireless, mobile data, or other sources, automated programs may be scanning your connection for vulnerabilities. These programs seek to exploit known flaws in the software that connects you to the world. If such a program finds that you are vulnerable, it reports back to the person who launched the scanning program that you are vulnerable and that person may choose to breach your network. Once your system is compromised, the hacker may have access to all the information on your network or computer (credit card information, in particular), use your system as a base to attack other systems, use your system to store hacker tools or pirated software or, delete all of your data. It is critical to remember that this kind of thing *happens every day*.

Keep in mind also that anything can be hacked. Hackers usually look for easy targets, and Jewish institutions should be especially concerned: because of who you are, you may be specifically targeted for electronic harassment.

Your system is also vulnerable to infection by malicious computer programs. These programs are indiscriminate and generally enter the system by inadvertent user action. Most data breaches or website defacements happen because of outdated website coding software, lax security by website administrators or hosting companies, malicious employee activity, or "phishing" scams that load dangerous software or fool users into divulging passwords. For specific examples, please refer to the section on common attacks and preventions listed later in the chapter.

The first step toward reasonable network security is a risk assessment. Here are some questions that will help you conduct a risk assessment.

## Identify Critical Information

- What do you have stored on your computers that, if compromised, could hurt or embarrass you or the people and organizations that you care about?
- Who within your organization has access to this information?
- Who has the authority to change or delete entries?
- Is the information accessible by outsiders or by employee using remote access?
- Do you have a policy regarding creation of backups for your critical data?
- Does your backup system work?
- Where are the backups? Who has access to the backups?

## Technical Issues

- Do you have a Web site? Is it hosted on a server or located on a private computer?
- Is there anything confidential that is also stored on that computer?
- Are the computers in your institution interconnected on a network?
- Do you have a firewall? Do you have active and updated antivirus programs?
- Do you allow for remote access?

## Policies

- Do you have a password policy?
- Do you have a policy regarding security steps to be taken when someone with significant access to your confidential information leaves your organization?

- Do you have a policy regarding privacy, confidentiality and network monitoring?

As you can see, addressing these questions focuses more on people than on technology. For the most part, humans, and not technology, are the weak link in the security chain. Technological tools are available to help enforce a security policy, but the policy itself is aimed at human behavior.

### Prevention, Detection, Response

Now that you have determined what information is critical and should be confidential, the question arises, how can I protect it?

## Prevention

Prevention consists of enforced policies designed to keep your network relatively secure and your confidential information confidential. Policies for prevention include:

- All employees should undergo background checks. Depending on the population you serve and the perceived level of threat, such a policy might also be extended to unknown interns and volunteers;
- Development of policies to determine who has access to sensitive information and at what level;
- Password policies; A properly configured firewall; Active antivirus protection;
- Advising all with access that their activities on the computer network are not private and may be monitored and that their workstations are subject to search without notice (or in accordance with federal, state and local law);
- Limiting or eliminating remote access (if limited, use a virtual private net-work or other secure communication channel); including access by mobile devices if applicable
- Backup management policies; and
- Termination policies.

## Detection

Detection can be proactive or reactive. Most proactive detection systems are beyond the financial resources of the readers of this manual. They include commercial intrusion detection systems and other software that can issue an alert when particular events occur. The software involved ranges from relatively inexpensive to very expensive but the real issue is the expense of having someone monitor the alerts that crop up. There is no point in having a burglar alarm that rings where no one can hear it.

A less expensive option would be detection tools to help recreate the security event and determine the source of an attack. Your server software should have an audit feature; turn it on and create regular (daily) backups. In the event of a security breach, the logs may help to determine the extent of the damage and the source.

Any computer system connected to the Internet has logs kept by the host or Internet provider of what outside sources visited or attempted to access the website or computer system. Unusual activity that may be indicated in these logs may be an early warning of attempts to probe a system for weakness. Server logs and IP logs, where available, should be reviewed regularly for unusual activity.

## Response

Response is itself a three-part process: *mitigation*, *remediation and investigation*. The level of response depends upon what has happened. If your donor list has been compromised and the donors are now receiving threatening electronic communications, a full-on response, including contacting the law enforcement and FBI cyber-crime specialists (http://www.ic3.gov/default.aspx), is required. In a situation where an employee has gained unauthorized access to another employee's electronic mail, the response may be much more limited.

You should have a plan that makes it clear who determines whether an event has occurred, categorizes the severity of the event and decides on the level of response required under the circumstances. It is a human and not a technical issue although technology, like computer forensics, can be brought to bear on the problem.

### Practical Approaches

We will now turn to the more practical issues of prevention, detection, and response.

## Practical Prevention

Computer security incidents will happen. If your computers are connected to the Internet, the risk is from outside and inside. If you are not connected to the Internet, your risk is limited to insiders.

Connecting to the Internet allows for theft to occur from outside of your walls, but the greater risk posed by an Internet connection is from malicious programs. These programs may not be targeted specifically at you. They are designed to search for and exploit vulnerabilities in computers connected to the Internet. There are, however, simple and inexpensive methods to prevent computer crime and vandalism. Following this advice will not make you invulnerable to computer attacks, but it will make it more difficult for an

attacker to reach you. Most attackers are not motivated enough to attack a well-protected computer and instead will move on to easier prey.

Here are the major examples of network use and ways to prevent computer security breaches:

**Email.** It is recommended that Institution officers, employees and key members should have email accounts and email addresses that are institution specific and not connected to private, home or business email accounts. These accounts should only be used for institutional business, community activity, and communication internally and externally.

- It is good practice that Institution email addresses should not reflect a person's name, location or any other online identity or presence (Facebook, LinkedIn, etc.)
- It is helpful to discuss and initiate a codified policy for the use of Institutional emails, who is entitled to have one and who is in charge of managing their distribution.
- When an email announcement is sent from an institution to a large list of recipients, the email addresses for the intended recipients should be placed in the "bcc" (Blind Carbon Copy) area of the addressee section of the email. This will prevent member names from being revealed if the email is forwarded to a third party by a member.

**Website.** An institution should always make the effort to have their Website hosted with a professional Web hosting company and avoid having the Website reside on an Institution or member's home computer.

- Institutions should meet or conference with their Web hosting service and ask about such things as active back-up of Website, what security measures do the hosting company use to prevent Denial of Service (DoS) attacks and unauthorized Website access. Also ask if they have a disaster recovery procedure that includes someone available as a 24/7 point of contact for emergencies.
- As with institutional email addresses, an effort should be made to limit and control the number of people who have access to Website administrator credentials or Webmaster permissions. Additionally there should also be a policy for password assignment and a schedule for changing passwords.

**Mobile Devices.** Due to the recent emergence and proliferation of smart mobile communication devices and mobile computing, there is at this time very little anti-virus or anti-malware protection for mobile computing devices. Mobile devices should only be granted access to institutional systems under the supervision of an experienced service provider, who clearly understands the security needs of a Jewish institution.

**Computer Systems.** It is in the best interest of any computer owner to be aware of who has access to their computer, the permissions granted to each account, who has system administrator authorization and who assigns passwords.

- It is a good practice to segregate general office and book keeping/member information to the greatest degree possible.
- If a computer system is connected to the Internet, an institution should consider using a primary carrier (Comcast, TimeWarner, Verizon, etc.) for Internet service. Companies who re-sell other company's services should be avoided where possible.
- It is always prudent to have active and up-to-date firewall, anti-virus and threat detection software.
- Although not all Websites or personal use of an institution's computers pose a problem, a basic "no personal use" policy is reasonable.
- As a general rule users should be discouraged from connecting personal devices, such as smartphones, SD cards, tablet computers and flash drives to institutional computer systems.
- Downloading of any material from the Internet should be closely supervised to avoid viruses and potential copyright infringement.

**Limit Access to Your Sensitive Information.** If your sensitive data, such as financial records, donor records and employee records, is located on a file server, set the access controls so that only the necessary personnel have access. Depending on the system, access rights, rights to modify, copy, print and delete records may be limited. If your data is on a file server, you probably have someone on staff who knows how to perform these tasks. If not, bring in a consultant to do it.

Even if the file server is only connected to other computers but those computers have Internet access, an attacker could compromise the file server by first compromising a computer with rights to access the file server.

If you have Internet connectivity, you may wish to consider purchasing a router/firewall combination. These hardware devices stand between your network, or your computer, and the Internet and make it very difficult to break in from outside. The best thing that they do is that they hide the Internet addresses of the computers on your network. Someone looking at your system from the outside will see only one Internet device, the router/firewall. The computers plugged into it are invisible and have addresses not accessible from outside. This is considered a minimal requirement for network security. It should be noted, however, that computer attacks have become increasingly sophisticated and firewalls are not guaranteed to protect your systems.

Many persons operating in an environment without a file server allow others in a network environment to have access to their files by enabling file sharing over a variety of options. An easy fix is to simply prohibit file sharing. If someone else needs to work on a report, give it to them on flashdrive or email it to them.

**Beware the Insider.**

- Use an operating system that allows for multiple users so that each person who must have access to the data has his/her own login and password. Advise your staff that password sharing is a serious violation of policy and is subject to disciplinary action. This will help ensure that should a security event occur, one will be able to determine whose login was used when the damage or theft occurred.

- Make sure that administrator privileges are limited to the one or two persons who must have them.

Employees, officers, interns and volunteers come and go. Do not provide them with administrative access to any machines unless they are coming on as system administrators. Spend the time to make sure that they only have access to data that is required for their job. Employees should sign a statement that advises them that they have no right to privacy in their electronic environment at work — that their files and communications may be monitored and searched without notice.

Remote access regularly is exploited for unauthorized access. Do not allow it unless necessary. If you have to, install software that provides for a Virtual Private Network (VPN) connection. At a minimum, this will limit your risk from an outsider taking advantage of remote capability to those outsiders who have stolen one of your VPN-enabled laptops.

**Passwords Are Not Security.** Passwords are part of a security plan but they can easily be compromised. At best, passwords prevent damage by the least skilled miscreant. The false sense of security created by passwords can be a bigger problem. Passwords need to be changed regularly and should be hard to guess. They should involve both small and upper case letters, numbers and alphanumeric symbols such as "!". Substituting a symbol for a letter does a lot toward making it more difficult for pass-words to be cracked.

**Pay Attention.** Oftentimes, in retrospect, it will be obvious that a computer security event has occurred. If a staff member attempts to log on to the network and is informed electronically that he or she is already logged on, this signals a problem. The solution is not to hit "OK" and continue. Employees should be advised to tell someone immediately.

## Practical Detection

Unfortunately, there is no easy and cheap method for detecting a security breach in a network. When data is copied and stolen, the original data remains unsullied and in place. Until the stolen data is exploited in some way or posted on the Internet, the owner may not know that it was taken. Similarly, Web page defacement may not be noticed until some customer or client calls you to report it. The point is that it is better to focus hard on prevention than worry too much about detection. Some preventative measures may also double as detection measures. Paying attention, for example, works just as well to detect an event as it does to prevent an event.

It also is useful to scan your system from time to time, to see what it is telling the world and to determine whether you are vulnerable in unexpected ways. There are a number of Web sites that will allow you to scan your system without charge. Try, for example, www.grc.com or the snoop test at www.anonymizer.com.[4] You may find that there are things that you need to do to shore up your system.

If you are interested in detecting an event and you have a technical person on staff, ask that staff member to enable logging in your firewall and check the logs from time to time. Once someone breaks into your system, they tend to stay awhile and come back for more. They often open up holes into your system that they can exploit later. Checking the logs for inappropriate connections is a good way to determine if you have an ongoing problem.

## Practical Responses

The trick to effectively responding to a network or computer security event is planning for it before it happens. Otherwise, the first response to learning that your computer system has been compromised is panic. As in so many other areas of security planning, the first order of business is to designate who the decision-maker will be in the event of a compromise. This is important because the level of response required depends upon the nature and significance of the event. For example, if your system has been infected with a virus or a worm, the response will be different than if your financial data has been stolen and deleted. In the first example, the virus needs to be eradicated and virus software updated. Corrupted data needs to be restored from backups (see below). In the latter, when your system has been trashed, you may decide that the offender be sought, and if identified, prosecuted. If such an event occurs, professionals will need to be utilized.

[4] ADL offers these two Web sites for informational purposes only and does not warrant the effectiveness or completeness of these Web sites or their services.

In the event of an attack on your system, you may wish to leave the computer unused in order not to lose possible evidence.

**Response Steps.**

- Determine who is in charge.
- Determine what has happened.
- Decide whether to preserve evidence or repair immediately.
- Document breach — especially if there are repeat offenders.

**Common forms of Cyber Assault and Recommended Responses.** Computer system intrusion can happen in a variety of ways: access in an unauthorized manner, by an unauthorized user, internally by a member of the institution or externally by the public.

- Advanced software can alert a system administrator if an unauthorized access has been attempted. Older systems may require a regular manually review of computer logs to detect unwanted access.
- Computer logs and advanced software, if properly configured, can indicate which computer files, if any, have been accessed. A policy should be established to inform members if files containing personal or sensitive information have been exposed. It is likely best to err on the side of caution in such situations.
- As soon as a system intrusion is detected the system administrator must be contacted immediately. Subsequent contact to law enforcement and FBI (http://www.ic3.gov/default.aspx) computer crime specialists is recommended.

**Website Hacking.** Website hacking can take a number of different forms and can happen for a variety of reasons. For this document we are defining a hacking as activity in the secure section of a Website that is *not* the result of action by an authorized individual. How the hacking occurs is secondary, here we are discussing what to do afterward.

- We suggest contacting the hosting company for the Website as soon as the incident is discovered. The hosting company will need to preserve a copy of the hacked page(s) and copies of all relevant server logs. The hacked page(s) need to be removed as soon as possible in case malware is involved and also to limit the hacker's usual main objective – to gloat.
- Report the event to the police and FBI (http://www.ic3.gov/default.aspx) promptly. Provide them with a copy of the material left by the hacker especially if it involves threats or hateful language.

- Restore the Website from back-up copy of the Website, but only after the hosting company or ISP acknowledges the issues relating to the hack have been addressed.

**Distributed Denial of Service Attack (aka DoS Attack).** DoS attacks are the simplest and most common form of cyber-attack. A DoS attack is a coordinated effort by a group of computers to request access to a Website. This creates a situation where no one can access the Website or that the contents are delivered very slowly. In many cases a Website hosting company will shut down a Website temporarily rather than create a problem for their other customers. If a Website is the potential target of attacks, the Website hosting company should be made aware of the situation in order to help offer solutions.

**Backups.** The key to any remediation of the system is the quality and age of your backups. To protect irreplaceable information it is essential to back up your data on a regular basis. Remember that if your system gets trashed by an electronic virus or a human — or even by fire, a lightning strike, a faulty hard drive or a spilled cup of coffee — you may lose all of your data.

## Final Word on Computer Data Security

The information here is merely an overview of what is required for network security. In a small office environment, particularly one with limited resources, protecting electronic assets is an important issue. Ignoring the issue is not a solution. At a minimum, you need to:

- Answer the questions posed earlier in this chapter and *remedy responses that are problematic*. Employ as many of the preventative steps as possible.
- Establish and enforce a backup policy.

## Web Site Sensitivity

It is understandable that one wishes to place a great deal of information on the Web. We often wish to highlight programs, staff, events, our schools and other items dealing with our agencies. And we often do this without regard to the possible consequences that may face our staff, our visitors and our constituency.

However, given that the Web is known for both searching and archiving, what goes on a Web site is both *permanent* and *public*. You can never recall information once it is released onto the Web.

### A Note on the Potential Harm of Posting Information on the Internet

*The harm that too much information can cause ranges far beyond its use by an anti-Semite; the harm caused can span the entire range of human cruelties*. Posting too much information on the Internet creates the potential for harm. For example, abusive spouses may use information posted in an online directory to hunt an ex-spouse and those who wish to harm children may use pictures and accompanying identifiable information to make an approach to a child. Furthermore, an anti-Semite can use the Internet for his or her own nefarious purposes: an online calendar or school opening and closing times can help him or her plan an attack for a time when no one is there, or, worse, for when there are people present.

## Information Controls

Because of the attendant dangers, we urge institutions to be prudent and exercise caution when posting information online. We suggest the following.

**See section on event planning.**

- No last names (e.g., John Smith will run the *oneg* on Friday) or other personally identifying information without express consent from the person.
- If and when you post photos of children, do not identify them by name (even in promotional material about your school and other services).
- Place calendars in a password-protected section; however, even this is minimally secure. While we do not recommend using the Web as a calendaring device, if you decide to use the Web for calendaring, ensure that you treat the event as a public or open one and adjust security appropriately.
- No membership directories.
- No donor lists.
- No floor plans or blueprints of the institution.
- No pictures of the institution that may be helpful in plotting an attack — too many viewpoints, pictures that include images of security devices, security officers and cameras.
- For reasons having to do with protection of the elderly against fraud, it is best not to publish information about congregant deaths.

These controls should be a part of the official policy of your agency or institution.

# Explosive Threat Response Planning: Bomb Threats, Mail Bombs, Truck Bombs and Suspicious Objects[5]

This chapter will help you develop an **Explosives Threat Response Plan,** dealing with **Phone Threats, Mailroom Security, Suspicious Objects** and **Car/Truck Bombs.** As with any aspect of security planning, assistance from professionals is strongly advised.

## Telephoned Bomb Threats[6]

The bomb threat is an all-too common form of harassment against communal institutions. Responding to such threats requires careful planning and rigorous practice. This chapter will guide you through some of the key elements of an Explosive Threat Response Plan (ETRP). It deals exclusively with explosive threats that are telephoned in or devices that are discovered; other sections of this booklet deal with mailed explosives.

There are essentially five stages your ETRP should address:

1. *Pre-threat*. Physical security, planning and practicing.

2. *Receipt*. The immediate response of personnel receiving a threat.

3. *Evaluation*. The point at which the threat is evaluated.

4. *Response*. Setting in motion an organizational response, from ignoring the threat to searching for a device to evacuating the building.

5. *Information and Post-Incident*. How the organization handles everything from informing constituency of the status of the incident, to how an organization recovers from disaster, to post-incident review.

---

[5] While this entire booklet deals with general security guidelines, it is worth mentioning that this chapter deals only with the outlines of an Explosive Threat Response Plan and offers general guidelines only. The ultimate decision on how to handle any explosive threat must be made by the individual responsible for the threatened facility. However, for the vast majority of institutions, we recommend immediate evacuation upon receipt of a threat.

[6] This section adopted from Bureau of Alcohol, Tobacco and Firearms, Bomb Threats and Physical Security Planning, ATF P 7550.2 (7/87)

# PRE-THREAT

## Physical Security

**It cannot be overstated that the best way to secure your institution from explosives is to have an adequate physical security plan in place.** By taking all responsible steps to prevent the introduction of an explosive into your environment, you markedly increase your institution's security. The first step in creating an ETRP is having a physical security plan that will help prevent the planting of a device. Of course, since no physical security plan is foolproof, it behooves even the most secure institution to have an ETRP as a back-up.

### Some Tips on explosive-specific physical security

- Offices and desks should be kept locked, especially those that are unused.
- Utility and janitorial closets should remain locked at all times, as should access to boiler rooms, mail rooms, computer areas, switchboards and elevator control rooms.
- Identify and secure potential hiding spaces for explosives. It is important to note that a device does not have to be large to cause severe physical as well as psychological damage.
- Trash receptacles, especially dumpsters, should be kept locked, inaccessible to outsiders and/or far away from buildings. The areas around these items should remain free of debris.
- Cars and trucks should be required, where possible, to maintain a safe setback from the facility. If no parking setback is possible, consider allowing only properly identified vehicles owned by staff or leadership to park closest to buildings.
- Shrubs and other plants and trees should be trimmed so as not to provide a hiding space for explosives.

- Employees should be encouraged to maintain tidy work areas so that they or their co-workers will notice if something is out of place.
- Flying glass is a grave source of danger in the event of a blast. Consider minimizing glass panes or coating with shatter-resistant film.
- More than one exit may be damaged in a sufficiently large blast. Map out alternative escape routes.
- Examine your local area to determine if you are at risk from a neighboring institution that may be targeted. Other Jewish institutions, political offices, medical facilities where abortion services are provided and corporate offices are such possibilities.

In order to design an effective ETRP, you must understand precisely how your local law enforcement agency will respond to explosive threats. In some areas, the police (or explosive unit) will not respond to such a threat until a device is discovered. In other areas, the police (or explosive unit) may respond to a called-in credible threat, but will not search a facility without a staff member present. This information is absolutely critical to your planning.

## Creating the ETRP

As discussed elsewhere in this book, planning includes assessment, plan creation and implementation. It is worthwhile to review these steps, but we encourage you to re-read the chapter on creating a security plan specifically with your ETRP in mind.

- Assessment includes marshaling all of the information resources available to better understand your institution's risk and realities.
- Planning includes many elements, but it is critically important to bring your local police and explosive squad unit into the picture (reminder: you may not have access to a bomb squad. Your local police department or ADL Regional Office may be able to help you reach them).
- Implementation will be discussed in greater detail below. However, without ongoing role-playing various scenarios, drills and reevaluation of your plan, your plan becomes stale and loses considerable value.

- Once you have developed a plan, it is essential that all personnel who need to implement it have copies and are trained. We suggest creating a checklist which will guide all parties through their required steps.

### Some basic considerations for the ETRP:

- Determine to what extent a bomb squad is available to you and at what point they will assist you.
- Set up a chain of command.
- Establish procedures for setting up a command center, both during and after business hours (see below, in "Evaluation and Decision" on page 55).
- Determine what primary and alternative communications are available. **Important: cell phones, cordless phones and walkie-talkies (any two-way radio)** can detonate a device. Thus, do not use such modes of communications during an explosive-related emergency. Alternatives include hard-wired intercoms and bullhorns.
- Clearly establish how and by whom an explosive threat will be evaluated.
- Establish procedures to be undertaken when a threat is received or a device is discovered.
- Provide an evacuation plan with enough flexibility to avoid danger areas, e.g., the ability to redirect an evacuation if a device is found in a stairwell.
- Designate and train search teams well in advance of a problem.
- Establish procedures to assign search patterns and track the progress of search teams.
- Establish procedures for a search team to record where they have located a device and a method for leading an explosive squad to the site.
- Have building plans readily available.
- Establish simple procedures for the recipient of the threat. The sample form attached to the end of this document will help. Note: anyone who answers outside phone lines needs to be aware of these procedures.

- Review your physical security plan in conjunction with the ETRP.
- Critically, know your facility. Know what belongs and what does not and be ready to walk through the facility and help police know the difference.
- In the event of a detonation, after the immediate emergency has passed, you will need to consider plans for continuing your operations. Having insurance information, lists of vendors and constituents and data-recovery capabilities can be very important to that end.

### Practicing

As just discussed, a stale plan loses value. **It is of utmost importance to role-play, drill and reevaluate your plan at several stages**. Role-playing involves the participation of all decision-making personnel who would be involved during an explosive threat scenario, talking through situations and variations on those situations to determine if the organization's ETRP is both comprehensive and complete.

Fire drills are often mandated by law or insurance carriers. They are a good way to practice your communication and evacuation plan. Adding explosive drills to the mix may require practicing search techniques, establishing a command post, etc. **There is very little substitute for actually moving through your institution and getting a sense of how your plan works during a real-time exercise.** Practice may not make perfect, but it will help get some of the kinks out of the system and will help turn your paper document into a real plan that people can use in an emergency.

Remember: evacuations due to bomb threats are very different from those initiated by fire. At a minimum, one needs to evacuate farther from the building and be sure that one does not evacuate into an area where a secondary explosive device or other danger awaits.

## Receipt of Phoned-in Threats

In this section we will deal with the receipt of phoned-in explosives threats. Mail threats are treated elsewhere.

The first step in developing a response plan for receiving an explosive threat is to meet with your local police department or explosive squad. They should be able to tell you what information they want the threat recipient to collect.

Do:

- Remain calm. A calm response may help in getting important information from the caller and it may provide the person making the threat with a human face to the situation.
- Do not irritate or insult the caller.
- Try to have a second person listen in on the call. A covert signaling system should be implemented or a recording device installed.
- If possible, the threat recipient should not hang up after the call. One suggestion: put the line on hold, and use another line to initiate emergency procedures.
- Keep the caller on the line for as long as possible. Consider asking the caller to repeat information.
- Try to recapture every word spoken by the caller. Use the checklists provided below, but also try to take detailed notes *even if there is a recording device installed*. Equipment failure and human error are always a possibility with such equipment.
- Remember: during a bomb threat, use no devices that generate radio signals, such as cell phones, cordless phones, walkie-talkies, etc.

**Remember, anyone who answers an outside line should know this.**

**IN AN EMERGENCY use an Explosive Threat Call Checklist like the one provided in this booklet.**

Information to be sought by the threat recipient includes:

- If the caller does not provide it, ask the caller WHEN the explosive will go off and WHERE the explosive is located.
- Inform the caller that the building is occupied and that the detonation of an explosive could result in death or serious injury to many innocent people.
- Pay particular attention to background noises. Listen for the sound of a motor running, music playing, and any other noise which may provide information about a caller's location.
- Listen closely to the caller's voice. Record that information on the Explosive Threat Call Checklist.
- REPORT the information immediately.
- Remain available for questioning by law enforcement.

# Evaluation and Decision

## Command, Control and Communications

In any emergency, firm lines of command, control and communications are essential. Among the considerations you may wish to discuss with a security professional are:

Command, control and communications form the backbone of an ETRP, indeed, of any security plan. 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 them. It is also important to recognize that a designated decision-maker 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 you to quickly establish a clear chain of command in light of the day's staffing and attendance.

You should consider establishing a command center, the place where your 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. A second, alternate site may be necessary if the first site is unsafe or unavailable. Ensure that your command center can be up and running both during and after business hours.

- Get your command and communications centers (primary and secondary) up and running.
- Determine likely locations. Produce a master target list and use it in light of the information received in the threat in order to narrow a search.
- Determine procedures to establish search patterns and track the progress of search teams.
- Have building plans readily available.
- Have a roster of all necessary telephone numbers available.

## Decision Point

There are three choices the decision-making authority has after an explosive threat is received:

- Evacuate immediately
- Search and evacuate as needed
- Ignore the threat

The threat should never be ignored.

**All things considered, immediate evacuation is likely to be the wisest choice barring some unique aspect of your facility (e.g., a hospital).** While such a policy may lead to a loss of time and/or subject the institution to copycat threats as a means to interrupt business and for other forms of harassment, given the potential risk to human life and safety we believe immediate evacuation is, by far, the safest policy. Also, you can reexamine your policy if you later determine that it is being used for harassment.

Other reasons favor an immediate evacuation policy:

- First, you avoid having to make a very difficult decision under extremely trying circumstances.
- Second, while the statistical probability is that any threat is false, such threats have led to explosives being discovered.
- Third, your employees and constituents will appreciate your caution — and may react badly to your institution's ignoring a threat.
- Fourth, in the absence of an evacuation, an explosive threat caller may feel ignored and choose to escalate.

## Immediate Evacuation

You must ensure your staff is trained to conduct a safe evacuation in advance of the need.

1. Call 911.
2. Notify all persons in the structure.
3. Conduct evacuation in an orderly fashion.
4. Be flexible; have alternate routes known in case of unexpectedly blocked areas.

## Tips for evacuation:

- Evacuation plans should account for several different scenarios and route blockages.
- Groups should be led by someone familiar with the path of egress. That person should look for obstructions and explosives while leading others to safety.
- Safe evacuation distances vary; however, one rule of thumb is if you can see the suspicious device or vehicle, you are too close. It is always better to be farther away than to remain unintentionally in a danger zone.

- It is useful to have a place to bring evacuees in the event of inclement weather. Arrangements with another facility in your area (a school, hospital, nursing home or a supermarket) will allow you to establish a destination for your evacuees. Some institutions have established more than one safe location increasingly far from their facility (one block, five blocks, 25 blocks). In some rural or suburban areas, there may be no large facility for evacuation; a friendly neighbor's house may be the best place to bring young children.

- There is also a risk from secondary devices (explosives left outside a facility to harm evacuees). At the very least, try to ensure that evacuees are moved a sufficient distance away so as to avoid such a secondary danger.

- Children and other persons in need of supervision and aid may raise special evacuation concerns and may have special needs upon exiting the building. While this is discussed in more detail in the section on schools, consider having "to go" bags which contain items needed for those who would face extra hardship during an extended evacuation.

## Search and Evacuate as Needed

After a threat, your institution will likely have to perform a search for the explosive with the help of the local police or explosive squad. Repeating what we discussed earlier: an ETRP requires that you understand precisely how your local law enforcement will respond to explosive threats. This information is absolutely critical to your planning.

**Tips on conducting a search:**
**The police might insist that you search your own facility; you need to make a decision about whether you will do so and whether it is safe for any searchers to remain inside.**

- Everyone should check over his/her own workspace to ensure nothing has been hidden in the work area if you believe it is safe to do so.

- It is recommended that you use more than one person to search every space, even if that space is small. (Ideally, several teams of two should be your primary searchers.) Teams can be made up of supervisory personnel, area occupants or specially trained search teams. While the first two lead to the quickest search, the latter is ultimately safer and more thorough.

- When searching a room with two people:

    - The two enter a room or area.
    - Carefully move to various parts of the room and listen quietly for the sound of a timing device. Understand that that there is a great deal of noise in typical buildings.

  - The searchers typically divide the room into four heights: floor to hip level, hip to chin, chin to overhead and, finally, ceilings and fixtures
  - Starting at a single point and standing back to back, the searchers begin to walk the circumference of the room looking for devices in the first height range. Examine everything, including carpeting, ducts, heaters, etc. When the searchers meet, they should proceed to the center of the room and search objects and furniture there.

- Repeat these steps for each of the next three levels.

- Finally, check for devices that may be hidden in false or suspended ceilings, and check for lights, building framing members (e.g., rafters, studs), etc.

- Once a room or area is searched, have a way to let others know it is searched. One common method is to mark the wall with tape or hang a "search complete" sign.

- The outside of your building must be searched. Examine:
  - Along walls, looking behind and into bushes.
  - Inside any enclosure, including planters, sheds, etc.
  - Under and inside every vehicle parked close by. Look for a vehicle that sits heavy on its springs, etc. Identify and examine vehicles that do not belong. (See the chapter, "Security for the High Holy Days and Other Special Events")

- Teams or your general staff should be trained in this technique.

- Previously, we suggested keeping unused offices and spaces locked. If you have reason to believe that these spaces may have been compromised, you must search these areas. Your command center should have keys or access cards for all areas.

## Discovery

It is absolutely critical that personnel involved in explosive searching must understand that they are only to look for and report suspicious objects. **THEY ARE NOT TO TOUCH, MOVE OR JAR ANY OBJECTS OF CONCERN.**

- Evacuate the building.

- Searchers must be able to:

  - Report the location of the device.
  - Give accurate instructions as to how to locate the device.
  - Describe the device.
  - Be available to emergency responder units.

- **Note:** Open doors or windows to minimize damage from blast and concussion.

### IGNORE THE THREAT

**NEVER IGNORE THE THREAT. THE CONSEQUENCES OF IGNORING SUCH THREATS ARE UNACCEPTABLE.**

### POST-INCIDENT

See the chapter on Post Incident Reviews later in this manual.

## Arson and Synagogues

### Arson Prevention Basics

Effective physical security is critical to deterring arson: good locks, good lighting, etc., as discussed in the physical security chapter, are all important. In addition to the tips discussed elsewhere in this guide, consider the following, even if they are not mandated by law:

- Smoke detectors, fire alarms and fire suppression systems
- Developing a relationship with your local fire department, including sharing and discussing site plans
- Working on your relationships with neighbors — they will be in a good position to notice and report suspicious activity
- Annually reevaluate insurance of buildings and contents
- Store fire extinguishers at designated locations; make sure that staff knows where they are and how to use them
- Have heating and air conditioning systems checked semiannually
- Store hoses at external spigots
- Ensure that electrical service is adequate for current demands
- Clean away all clutter, both inside and out
- Store all flammables, paint, gasoline, mowers, etc. outside in a locked storage area away from your main building.

## Protecting Your Torah

It is important to protect your Torahs from both water and fire damage, either by storing them in a fire- and water-resistant location (or creating an ark that is fire- or water-resistant), designing your sprinkler system so that it does not get the ark wet, or using a chemical fire suppression system that does not use water. It is critically important to negotiate the insurance of your scrolls to include your understanding of what a total loss might be: if you believe that a Torah is damaged beyond use and is thus a total loss if one letter is erased through water, you should work that out with your insurance carrier in advance of any problem.

## Mail Room Security[7]

Mailroom security follows the same five-part model as above.

1. *Pre-threat*. Physical security, planning and practice.

2. *Receipt*. The immediate response of personnel receiving a threat or noticing a suspicious item.

3. *Evaluation*. The point at which the threat is evaluated.

4. *Response*. Setting in motion an organizational response.

5. *Post-Incident*. How the organization handled everything from informing constituency of the status of the incident to how an organization recovers from post incident.

### PRE-THREAT

The first key to a mailed hazard response plan is to channel all mail and packages through a screening process, to avoid any letter or package escaping formal scrutiny. This includes items received through the postal service, overnight carriers and couriers. It is preferable that one or two individuals deal with mail so that they become experienced with letters and packages.

To establish a mail screening program:

- Conduct a vulnerability assessment to determine if your organization or a particular employee is a potential target (see "Introduction: Security Planning" on page 4).

[7] Adapted from United States Postal Service, Mail Center Guide, Publication 166.

- If your institution is large enough, appoint a mail center security coordinator and an alternate to be responsible for the developed plan and to ensure compliance with it.
- Establish direct lines of notification and communication among the mail center security coordinator, management and your general security office.
- Develop specific screening and inspection procedures for all incoming mail or package deliveries. At the least, develop a method for ensuring that all packages and mail are examined by someone who is able to evaluate them.
- Develop specific mail center handling techniques and procedures for items identified as suspicious and dangerous.
- Develop verification procedures for confirming the contents of suspicious packages encountered through the screening process. If you receive a suspicious package, it may be useful to call the addressee to see if he/she is expecting something.
- Establish procedures for isolating the suspicious package. At the least, identify an isolated room or area in which to place suspicious items until law enforcement arrives. The room, ideally, should have windows that open in order to allow fumes or the pressure wave from an explosion to escape. (Do not place the package in cabinets or drawers)
- Conduct training sessions for mail center, security and management personnel to ensure that all phases of a mail screening program work.
- Conduct training for all employees of the institution to look for suspicious mail and packages.
- Conduct unannounced tests for mail center personnel.

When conditions warrant and depending on the level of risk your institution faces and the resources available to it, you may wish to set up an isolated screening room and have your screener wear rubber gloves and a HEPA face mask to prevent bio-logical or chemical impact.

## Receipt and Evaluation and Decision

All letters and packages should be hand-sorted and screened.

One indicator of a suspicious package or piece of mail includes inappropriate or unusual labeling, such as:

- Excessive postage
- Misspelled common words

- Unusual addressing, such as not being addressed to a specific person or the use of incorrect titles or titles with no name
- No return address; unusual return address; mismatch between return address and city/state listed in postmark
- Markings indicating that item was mailed from a foreign country
- Markings like "personal", "confidential" or "do not X-ray" which serve to restrict screening of mail
- Threatening or otherwise unusual language on envelope/parcel or in contents
- Mail whose source cannot be verified

Other indicators include an unusual or inappropriate appearance, including:

- Powdery substances felt through or appearing on the item
- Oily stains or discolorations on the exterior
- Strange odors
- Excessive packaging material, like tape or string
- Lopsided or bulky shape of envelopes or boxes
- Protruding wires, or exposed aluminum foil
- Excessive weight

**Note:** Do not presume that a mail bomb will necessarily meet any of these criteria. Your observations and intuition are two vital elements in identifying suspicious packages. Since the most likely person to identify a mail bomb is the intended recipient, all employees should also receive training about what to look for.

## Response

Depending on the risk identified, once a suspicious letter or package is identified, a number of steps should take place.

### Explosives

- Call law enforcement.
- Handle the mailed package with extreme care.
- Do not shake or bump.
- Do not open, smell, touch or taste the package or its contents.
- Isolate the package.
- Enact internal emergency procedures (e.g., evacuate).

When isolating the package, it is best to place the container in a room with open windows (to deflect the blast). Do not place the container in a room that has glass walls or doors.

If you have reason to suspect that the suspicious package may contain biological, chemical or radiological hazards (e.g., it is warm, has strange odors or it contains suspicious powders), then consider the following additional precautions:

### Radiological Hazards

- Call emergency responders.
- Limit exposure — do not handle.
- Distance yourself and others (evacuate area).
- Shield yourself from object.
- Enact internal emergency procedures (e.g., evacuate).

### Biological or Chemical Hazards

- Isolate — do not handle.
- Distance yourself and others (evacuate area).
- Enact internal emergency procedures (e.g., evacuate).
- Call emergency responders.
- Wash your hands with soap and warm water.

Make certain you articulate clearly to the 911 operator that you have reason to believe you are dealing with a chemical, biological, or radiological situation.

*** No staff or visitors should leave the area until they have been cleared to do so by emergency responders.**

## POST-INCIDENT

See Post-Incident Reviews later on in this manual.

## Truck and Car Bombs

Without extensive physical alterations and an extensive security program, defending against truck and car bombs is extremely difficult. Nevertheless, individual awareness as well as those physical security precautions your institution may take represent an important improvement over doing nothing at all.

Truck and car bomb prevention is a matter of physical security first, search and evacuation second. Your key defense is to exclude potentially dangerous vehicles from your institution.

Ideally, all vehicles entering your facility's grounds should be scrutinized before being admitted. While it is much less than ideal, it is still significantly better than doing nothing if you scrutinize vehicles once they are on the grounds or parked.

Truck and car bombs might be identified by the outward appearance of the vehicle and the behavior of the driver. Suspicious facts include, but are not limited to:

- The person driving the vehicle does not enter the facility, but rather runs or walks away. The car or truck appears to be sitting very low on its springs, indicating great weight.
- The car or truck is parked illegally (or too) close to your building. Your facility should restrict parking closest to the building. In an urban environment where on-street parking is close to the facility, consider making a request to the local police department for no-parking designations. Your institution may consider adding physical barriers (cement barriers) between the street and your facility.
- Note that older cars and trucks are more likely to be used in a car bombing (as are rental vehicles). Be wary of any type of vehicle that appears to have been abandoned (e.g., inspection sticker, registration or license plate expired or missing, etc.).
- Information had been received from the FBI that al Qaeda operatives discussed attacking Jewish institutions using bomb-laden fuel trucks. **Institutions should be extremely alert to fuel and tanker trucks parked near their facilities.** The police should be called immediately if any doubt exists about the legitimacy of such trucks (e.g., no fuel delivery expected or such deliveries are not expected at your institution or are atypical of the neighborhood).

None of these behaviors are perfect indicators of the potential for violent behavior — and many are consistent with perfectly innocent behavior — however, they are clues worth considering.

* Observation and rapid response are key to dealing with suspicious vehicles.

You should think through how you will respond to the observation of a suspicious vehicle well in advance of the discovery of one. Suspicious vehicles may require immediate action, including evacuation and calling emergency services. Remember, it may be appropriate to evacuate to a location that puts another structure between you and the explosive threat. Discuss this possibility with your fire marshal or bomb squad.

### Incremental Steps for Truck Bomb Security

1. Seek to restrict parking closest to your buildings (perhaps no parking at all or limited to staff/key lay leader vehicles). You may choose to use a windshield identification sticker to determine quickly who belongs and who needs further scrutiny.
2. Train staff and security to be aware of the possible appearance of vehicles used in these incidents.
3. Use barriers, gates, etc. to prevent access to the facility by non-authorized persons.

## Unwarranted Interest in Your Facility

Many terrorist organizations first engage in surveillance on their potential targets. You and your staff should therefore pay serious attention to anyone attempting to photograph or study your facilities — especially in the days and weeks leading up to the High Holy Days or other special events.

Someone examining your facility (or looking closely at the people arriving at or leaving from your building) should be cause for concern. If you spot someone you believe may be doing surveillance on your facility:

1. Call the police **immediately**. It is crucial that the dispatcher/911 operator be given **all** available information, starting with the fact that the location is a Jewish institution and its exact address and location. Other important items would include a description of the suspicious individual, approximate height and weight, what clothing he/she has on, type of car and license plate number if one is observed and any unusual characteristics that would make the person or persons easy to identify.
2. **Consistent with your safety and personal comfort level,** consider photographing the person doing surveillance. If the institution has video cameras that are actively monitored, make sure the operators know what to look for and to get film of the incident.
3. If the person leaves before police arrive, you may choose, **consistent with your safety and personal comfort level,** to approach the individual and inquire as to why he or she is taking photos of the location.

   You will have the benefit of placing the person "on notice" that his or her actions were observed. Get a picture of the subject/car as he or she leaves.
4. Even if the person leaves, police should be informed and given a report. If the responding law enforcement officer refuses to take a report, call ADL. Also, here is where preexisting relationships with police help: contact the person you already know. If a dispatcher does not consider this an emergency, inform him or her that you feel threatened and require assistance immediately.

5. Ensure that your staff knows all relevant facts and so can identify the person or persons if they return.

6. Your safety is of paramount importance. Remember: call the police first and act to take pictures, get license information, etc. only if you are confident that it is safe to do so.

## Suspicious Objects

Prior to the start of services or events and at the beginning of each day, ushers, security officers and others should walk the perimeter, including parking lots and, if possible, rooftops, as well as inside the facility. They should do this in order to refresh their memories as to what belongs and what does not. During the holiday or event, ushers and security officers should periodically patrol the facility.

If you come across a suspicious item:

**Leave it alone.** Do not move it or touch it.

**Establish Ownership.** Ask people in the immediate vicinity if they own it.

**Evacuate.** If you decide it may be an explosive device, evacuate the vicinity. *Rule of thumb:* after you have evacuated, if you can see the device, you are too close.

**Call Police.** But do not use a cell phone, cordless phone, walkie-talkie, or any other electronic device (bombs may be triggered by radio signals).

# Active Shooters[8]

An Active Shooter is an individual actively engaged in killing or attempting to kill people in a confined and populated area; in most cases, active shooters use firearm(s) and there is no pattern or method to their selection of victims. Active shooter situations are unpredictable and evolve quickly. Typically, the immediate deployment of law enforcement is required to stop the shooting and mitigate harm to victims. Because active shooter situations are often over before law enforcement arrives on the scene, individuals must be prepared both mentally and physically to deal with an active shooter situation. The following are generally accepted practices by Department of Homeland Security and other respected protective organizations that individuals should follow when reacting to or responding to an emergent Active Shooter situation.

### Procedures:

Each active shooter event is unique based on the specific nature of the event and circumstances surrounding the incident. Anyone who encounters a hostile person(s) who is actively causing deadly force or threatening the immediate use of deadly force within the facility should react in accordance with the following procedures depending on the situation. Regardless of the specific action that is appropriate for the situation, notification of law enforcement personnel is a priority and should occur as soon as possible.

## Potential Actions:

**Evacuate – (Get out)**. If there is a safe way to do so, evacuate the area immediately. It is always important when in a public area to know where the exit signs are. Pick the best route with cover or concealment, if possible. When possible, assist others to evacuate. Special considerations should be made for disabled individuals and others who may need assistance. Leave personal belongings behind, keep hands visible at all times and follow the directions of law enforcement personnel once outside.

**Shelter in Place - (Hide out).** If it is not safe to evacuate, take measures to protect your life and the lives of others. Seek shelter in a place where the shooter is less likely to locate you, and take appropriate measures to lock yourself in the area and/or barricade the area as necessary. Close all blinds, block windows, turn off radios and computers and silence cell phones, pagers and other devices that might make noise.

- **Hide** behind large items (i.e., desks, cabinets)
- Shelter behind fire walls if available
- Stay away from doors that can be easily shot through
- Make a plan if the suspect breaches the door---see Take Out section

**Call for Help (Call out):** As soon as possible, and when communication is feasible, contact the

[8]Prepared by the ADL's National Communal Security Committee

911 operator, the caller should provide the following information:

- Your specific location – Building Name and Office/Room Number
- Number of people at your specific location
- Injuries – number injured; types of injuries
- Assailant(s) – location, number of assailant(s), race/gender, clothing description, physical features, types of weapons (long gun or hand gun), backpack, assailant(s) identity if known, separate explosions from gunfire, etc.
- Announce the intentions and/or demands of the suspect(s)
- Demeanor of the suspect(s), (are they calm, agitated, angry, violent)

**Confront the Active Shooter (Take out):** As an absolute last resort, and only if your life is in immediate danger, attempt to disrupt the active shooter. Raise your voice to the active shooter and yell as necessary, act aggressively, commit to your actions and if necessary, throw items and improvise weapons. Disrupting the active shooter should only be considered when your life is in imminent danger, you cannot evacuate the area or shelter in place, and you are truly left with no other options.

During the course of an Active Shooter event, Public **Law Enforcement will be required to properly terminate the incident**. Some characteristics of Public Law Enforcement operations during an Active Shooter event include:

- Law Enforcement **must** assume that everyone is a threat to their safety
- Officers will proceed directly to the area in which the last shots were heard
- Officers arriving usually form into groups of four (4), in order to move to contact the active shooter
- Officers may wear regular patrol uniforms or external bulletproof vests, helmets, and other tactical equipment
- Officers may be armed with rifles, shotguns, and/or handguns
- Officers may use pepper spray or tear gas to control the situation
- Officers may shout commands and may push individuals to the ground for their safety

When dealing with Public Law Enforcement in Active Shooter event, one should be prepared to do the following:

- Keep your hands visible
- Be subjected to search
- Be escorted out of the building by law enforcement personnel – follow their directions
- After evacuation, be taken to a staging or holding area for medical care, interviewing, counseling, etc.
- Once you have been evacuated, you will not be permitted to retrieve items or access the area until law enforcement releases the crime or issues the ALL CLEAR sign

Facilities managers, site security, or leadership on site should:

- Contact the Police Department and transfer all gathered information to them
- Provide information on number of suspects, hostages, locations, injuries, etc.

- Monitor the CCTV surveillance systems to locate the suspects(s) and potential victim(s)
- Lockdown the facility (depending on the location of the suspect(s)). This will prevent newcomers from gaining access but will allow staff and patients inside to escape.
- Initiate an Active Shooter announcement by utilizing the overhead paging system, describing the location followed by instructions.
- Direct responding Law Enforcement Officials to the location of the incident, provide all known information about the incident and give them access cards, keys, and floor plans.

Deal with the aftermath. This including caring for victims and their families.

***See "Considerations for Schools and Summer Camps" for further discussion of lockdowns and evacuation pertaining to children.***

# Considerations for Schools and Summer Camps

By and large, the entire contents of this manual apply to religious schools and summer camps. However, some specific recommendations for organizations that deal with large numbers of children may be helpful.

## Schools

Hebrew schools and Jewish day schools represent a key arena of concern. Parents are keenly aware of the visibility of many of these schools and past targeting of Jewish institutions by those who would do harm by attacking our children. Therefore, pressure is brought to bear by parents — often in a highly emotional and unstructured manner — demanding that schools spare no expense to ensure the safety of their children. It behooves the principal/director, staff and lay board to consider the implementation of a serious, ongoing security program, if one is not in place, before events — which typically happen outside the institution — result in rapid, ill-considered and potentially costly steps.

This chapter will not focus on the cause and prevention of student-initiated violence. However, some of the items discussed may be applicable.

Everything we have said about building relationships with police applies here. Indeed, your location may be considered ideal for SWAT or other police training exercises.

## Physical Security

- Follow the steps discussed elsewhere in the manual. However, in conducting your assessment/audit, recognize that Jewish day schools and Hebrew schools are attractive targets to those who may wish Jewish communal institutions harm. They may also be targets of those who wish children harm in general.

- It is vital that all staff wear photo identification and that all visitors understand that visitors' ID must be worn without exception. There must be 100 percent compliance by all staff and visitors. Your institution should decide how that compliance is to be achieved. Failure to comply with the badge program diminishes, both in reality and in the eyes of key constituencies, the commitment of the institution to the security of those in their charge.

## Special Evacuation Concerns

- Understand evacuation protocols and the potential consequences if you choose to evacuate, such as the possibility that people may be directed into harm's way.
- You must provide for sufficient and age-appropriate supervision.

- Responding emergency personnel will need to know the numbers and ages of the children who are involved as well as the numbers of staff involved.
- An effective method of informing parents such as a telephone tree must be established to prevent panic on the part of parents hearing of an evacuation or threat.

Information for the telephone tree should be simple so as to avoid confusion and prevent muddling of information as it is passed from person to person.

Information should be calmly conveyed.

It is extremely important to let parents know where the children are being taken as well as when and how the children can be picked up.

**Note:** It is recommended that parents as well as staff be informed at the beginning of every school year of the evacuation plans an institution may have. Remember, rumor and innuendo are the most toxic forms of communication.

- Children, especially young ones, need to be taken to a sheltered environment. This can mean any location that is sufficiently far from your institution to ensure safety and is protected from the elements, etc. Examples may include a neighboring school, church, business, etc. You should, of course, make plans in advance to use such a facility. You may need to work to find a facility or combination of facilities that are open during your entire range of business hours.
- Be prepared for the possibility that staff or children may have to remain in that location for a number of hours. Consider the desirability of creating "to go" bags — i.e., disaster preparedness kits — for each classroom. Such kits could be readily taken by each teacher in any kind of emergency, particularly those requiring evacuation. Each bag might have a contact list for every child in the classroom (possibly along with a secondary, out-of-area contact) as well as some food, water and sunscreen. Such a kit would also be useful in lockdown situations.

## Lockdown or Shelter-in-Place

There are a number of reasons to initiate lockdowns, the most serious of which is the presence of a dangerous intruder where clear lines of safe evacuation are unavailable. Other circumstances include nearby police operations (which emphasizes the need for police to know your location and function).

A lockdown is a procedure whereby students and staff lock themselves into their offices, classrooms or other designated safe areas until danger has passed. In the event a lockdown is deemed necessary, the first step is to communicate that fact to staff and

students both in the classroom and throughout the campus. Students may be away from buildings, on a field, walking between classes, etc. They must be quickly informed and know to go into the nearest classroom or office. This presents a very confusing situation because (a) students who are unknown to a teacher may seek entrance into a class and (b) it may be difficult to account for students' whereabouts.

Some considerations:

- Can your rooms be locked from the inside?
- Do classrooms have windows large enough to present a danger to those inside the rooms? If so, is there a safe place to hide?
- Are there means of communication from classrooms to either the main office or the outside? If not, is there a procedure (possibly using colored cards) to inform police that all individuals in your room are safe or, conversely, that assistance is required immediately? The ability to convey such information may save lives. **WHATEVER SYSTEM YOU USE, IT MUST BE SHARED WITH, OR, BETTER YET, DEVELOPED IN CONCERT WITH LOCAL POLICE.**
- Are your rooms stocked for what might be an extended stay? Consider having water, food and perhaps some form of sanitation facilities available.

## Specialists

We have recommended elsewhere in this manual that you may wish to consult with a security professional. Your local public school district may have such a professional on staff or be willing to make a recommendation.

## Telling Parents About Security Plans

Parents often will ask in great detail about your security plans. The information provided to parents should be sufficient to calm concerns, but should not be so detailed so as to potentially impact the effectiveness of the security program. One way to manage this issue is to have a parents' committee that is fully briefed and able to provide assurances to other parents.

**Note:** Security plans and evacuation information should not be posted on Web sites or presented in other public arenas.

# Summer Camps

Summertime is not normally associated with security concerns, and those who work in — as well as those who attend — summer camps anticipate an enjoyable summer experience. And with some careful planning, summertime can remain enjoyable and safe.

The elements of a security plan for summer camp deal with:

- Physical security
- Information and communication
- Emergency planning

As in all institutions, one key element in security is the ability of management to establish command, control and communications in an emergency. While this is made more difficult given the nature of camps (they can be remote, or have children and adults outside playing on many fields at once, etc.), planning will make this possible and thus is an issue that camps can go a long way to meet.

## Physical Security

While most of the considerations about physical security addressed elsewhere in this book are applicable, summer camps have unique security issues.

### Day Camps

Day camps that are contained within the confines of a Jewish institution should be included in that institution's security plan. Even with such a plan in place there may be differences:

- Young people are outside far more often and for longer periods of time.
- Pickup and drop-off times may be more crowded.
- Other uses of the facility may be occurring simultaneously with camp.

At the very least, this translates into a need to exercise extreme caution when dealing with access to campers. Specifically, great attention needs to be paid to identifying those who are part of the camp program and challenging (in an appropriate way) those who do not belong.

#### Tips for all camps:

- Photo identification should be worn by staff and other adults permitted to enter the camp.
- If any identification is used by campers, it is very important that care be taken not to provide an opening for strangers to talk to the child, for instance, by broadcasting the child's first name (e.g., on a T-shirt or name tag).
- Staff should be carefully trained to report any person who attempts to make contact with campers.

- Though the majority of staff at a camp is young people, they can nevertheless play a role in challenging unknown individuals, even if it is only sending a fellow counselor to the administrative office to alert officials to the presence of an unknown individual.
- Counselors are rarely adults and yet are in a semi-supervisory role.
- Young counselors should not approach individuals but should maintain observation from a distance.
- The issue of how to alert responsible adults is one that must be worked out well in advance of the need and role-played with senior counselors.
- There should be at least one staff member within each group of campers with a cell phone available at all times, especially when campers are away from the main building (e.g., at a sporting field), to enable you to contact emergency personnel (without leaving the campers).

## Sleepaway Camps

Sleepaway camps have all of the challenges of day camps, multiplied by the fact that their responsibility extends 24 hours a day, seven days a week and that they are often located in remote settings.

Given the special nature of sleepaway camps, the following ought to be addressed, perhaps with the assistance of a professional security consultant. As we have said elsewhere, this is an important time to build relationships with local law enforcement. Indeed, it may be prudent to reach out to law enforcement during the "off-season," when these officials and the camp staff are all likely to be less busy.

The following are general considerations for camps, and we encourage that a security professional be consulted.

### Signs

- Posting. Institutions should clearly delineate their property with signs that indicate that trespassers are not welcome.
- Directions. Consideration should be given to the appropriateness of providing widely disseminated directions to the camp from public roads, especially if the camp is identifiable as Jewish by name.
- Internet. Information posted online should be very carefully screened. Consider not providing detailed directions to your camp.

## Access Control

- All visitors must be directed — both by signs and physical layout — to the main administration building.
- While badges or identification may be difficult for campers to wear at all times, all adults should be identified by badge, whether staff or visitor. Staff should at least be trained to direct visitors to the administration building, and depending on the age of the counselor, to take other steps as necessary.
- While it is unlikely that a sleepaway camp is fenced, there should be some method for keeping strangers and vehicles off the property, particularly at night. Consideration may be given to the possibility of fencing or patrolling the most sensitive parts of the camps, namely sleeping areas, and thus dramatically reducing the area that needs to be secured. Note: if a counselor is patrolling, serious consideration must be given to his/her ability to contact an adult counselor (e.g., a walkie-talkie or even an air horn).

## Mail

- Consider using a mail screening program (see section on mail screening). Some camps have found that the use of preprinted address labels facilitates that process.

## Lighting

- Areas and paths used at night should be well lit.
- Cabins should be well lit inside and out, front and back (especially if the cabin backs against the woods).

## Sleeping cabin security

- Cabins should have lockable doors and windows.

## Evacuation and lockdown procedures

- Evacuation procedures need to be worked out well in advance, especially if the camp is remotely located. You may decide that the best place to take children is to a main building, such as mess hall, recreation hall, etc. If so, consider ensuring that these buildings have sturdier locks and doors.
- Consider having the ability to institute a lockdown if necessary.
- See section on school evacuation.

## Training

- Staff must be included in training, practice and critique of a security plan.
- Refresher training is important as stale information is quickly forgotten.

## Information and Communications

There are two types of communications we will consider here: communication of personal information and emergency communications.

### Personal Information

All data pertaining to campers, employees, their families and their summer schedules should be treated as very sensitive information and kept in a secure and locked location. No information should be provided to any individuals, regardless of their story, about campers, employees, their families and their summer schedules. Such information should be distributed on a verified need-to-know basis only.

Again, camps should review the amount and types of information they post on the Internet. While it is understandable that camps wish to post as much information as possible on their Web sites, they should remember that once data is on the Web site it is impossible to ever "erase" that information from the Internet. If your camp uses a Web site to communicate with parents, consider a password-protected environment for all sensitive information.

### Cell Phones

Communications in remote locations can be very difficult and intermittent.

- There should always be at least two forms of communication available, typically a landline and a cell phone. Radios or satellite phones may be required, given the rural location of some camps.
- Sleepaway camps in rural areas — or if day camps are taking day trips into rural areas — may need to consider alternate means of communication, as cell phones may not work. Note: even if cell phones work on the main road driving up to a remote area, they may not work once off that road. It is important to let authorities in the remote area know when and where you will be and when you are expected to return as well as inquiring of them about communication in the remote area (there may be nothing). If there is no form of communication available, additional resources (medical, additional counselors, etc.) may be needed. At the very least, **do not publicize your trip beyond the appropriate camp family.** This may require a review of the camp's promotional literature and Web sites.

## Intra-Camp Communications

You should be able to communicate with all areas of your camp, regardless of the remoteness of the location of some facilities. Bear in mind that radios may not be useable if you are dealing with a bomb threat (radio signals may detonate a device). Consider using a public address system with a prearranged emergency signal or word, bullhorns, hardwired systems, etc.

## A Note on Emergency Planning

Again, a critical issue facing camps, especially sleepaway camps in remote locations, is establishing command, control and communications in an emergency. However, as the above discussions indicate, careful planning and consideration can go a long way to reducing this particular concern.

# DEALING WITH PROTESTERS AT JEWISH INSTITUTIONS

If your institution is the subject of picketing or protest, these guidelines may be of assistance. You should not hesitate to call law enforcement if you feel threatened in any way.

**Remember, every protest is different and not everything below applies to every situation.**

**Do not engage/debate protestors.** No one should speak to or respond in any way to the protestors, especially constituents or staff entering or leaving the facility.

- Educate your staff as to what you expect of them during the protest.
- We do not recommend holding counter-protests or educational events at the same location as, or close to, the protest. If you do so, you will bring protestors and counter-protestors together and dramatically increased security is likely to be warranted; speak to the police department about this. Also, even if you hold a counter-protest or counter-programming far away from the event, be prepared for those returning to your institution to have to walk past protestors.

**Contact the police department.** Notify the police of the protest.

- If you feel you need it (and err sharply on the side of caution here), ask for the police to send officers to the event to help maintain your security.
- Specifically notify the police if the protestors are on your property, are acting in a threatening manner, or use any violence or threats of violence. Do this even if the police are present.
- Discuss what permitting requirements may be necessary for the protest and any counter protests.
- Discuss the question of whether it is advisable to make alternative business arrangements for the day.

**Review and maintain your security procedures.** Ensure that your institution's rules and procedures for dealing with who gets into your facility are sufficient and are functioning.

- Practice (have a rehearsal) those rules with all staff.
- Be prepared to enforce those rules against potential protestors.
- Closely monitor who gains access to your facility.

- Ensure that all of your security devices are working and used (including door locks and alarm systems).
- Ensure that unused and unmonitored entrances are closed.
- Beyond access control, ensure that all of your institutions security procedures are sufficient and functioning.
- To the extent you are comfortable and feel safe doing so, it may be useful to video or photograph the protestor(s). Speak to an attorney about legal issues that may be related to this.

Additional information about security for Jewish communal institutions can be found at www.adl.org/security.

**Identify any vulnerable constituents.** Consider making an alternative arrangement, including using other entrances, driveways, etc., for children and/or guests who may be particularly vulnerable to anything the protestors do or say.

- Using entrances further away from the protest may prevent unwanted altercations/confrontations.

**Contact your attorney.** Reach out to your lawyer, who can help you understand where protestors may lawfully be and what rights you have. If you do not have an attorney, you might be able to find legal assistance through a local bar association.

- Protestors may have legal rights to protest near your facility; your lawyer can assist you with this determination.
- Protestors' speech and expression (including distributing flyers and other materials; chanting; holding signs; photos) may be legally protected speech.

**Consider Hiring Security Professionals.** A private security professional may offer guidance and personnel for dealing with a protest. Your local police department may also be willing to help in this regard. Please refer to the section of the manual entitled "Guidelines for Hiring A Security Contractor" for more details.

**Prepare a media response.** Protests are intended to attract the attention of the community and they may draw a media response. Should any media arrive, you might wish to have a short, prepared statement. We suggest not engaging the protestors on any level. Any such statement should be in simple, short declarative sentences. Craft your message before you are interviewed. Develop two or three key points and stick to them.

## Contact the Anti-Defamation League

- Your local ADL office can assist you with responding to the protest and dealing with media.
- ADL can also help provide education to you, your leadership, your employees and your constituents, especially if the group is an extremist or anti-Semitic group.
- ADL has online resources about security and extremists.

# Security for the High Holy Days and Other Special Events

The High Holy Days and other special events raise special security concerns for the Jewish community.

This chapter is designed to help Jewish community institutions prepare for holiday security in a calm and rational manner. Enhanced security does not have to come at the expense of an open and welcoming environment. And, it doesn't have to come at the expense of a balanced budget. It requires a commitment from their institution's management and constituency to make security a part of that institution's culture.

> Ideally, for security considerations to be effective, they should begin well in advance of the High Holy Days.

## General Recommendations

Several thoughts from earlier in this book bear repeating:

**Think Security.** Bear in mind that it is everyone's responsibility to keep a watchful eye on their community institutions. We must all take responsibility for security.

- **Leadership** should assess the risks and realities facing the institution and develop a security plan — seeking professional guidance, if needed. Of course, not all institutions run the same risk, but all run some risk.
- **Congregants and community members** must care about security and let others know that they do. Security procedures and your powers of observation are two of the most important assets you have.

Have a **security** (prevention) and an **emergency** (reaction) which includes (but is not limited to):

- Notifying and evacuating attendees, if necessary. Designate a meeting place to ensure that everyone is safe.
- Having a phone handy in case you need to call for help from outside the facility.
- Having a person in charge of security — and vesting that person with the authority to direct a response during an incident.

**See appendix on calling 911.**

Speak to local law enforcement about High Holy Day schedules and special events. Invite officers and the fire marshal to the facility for a security review — especially if the facilities are not the ones you usually use. Ensure that patrol officers are aware of the times during which

you will be holding events when large numbers of congregants will be walking on the local streets. Consider presenting copies of schedules for distribution at your police department's roll call. A previously developed relationship with law enforcement will help facilitate this.

Consider hiring outside security or off-duty police. Refer to the next chapter on Guidelines for Hiring a Security Contractor.

**Contact ADL for a threat assessment.**

**Coordinate ushering and security staff.** This is especially important when you are bringing in outside help for the holidays (e.g., off-duty police or a security officer). Note: ushers and security should be placed in reasonable proximity to each other so that ushers can quickly alert security to a problem.

- A facility should have as few entry points as possible (ideally, one). However, remember to obey all fire codes and ensure adequate routes for exiting the building.
- Ensure that existing safety devices are working and useable — especially if you are renting a facility. Video cameras should have tape, parking lot lights should work, etc.
- Ensure that ushers understand that they play a critical role in security matters (even where there is a security staff) as they are often used to control access to the sanctuary (e.g., by taking tickets) and are in a position to spot trouble early. Meet with your ushers prior to services to make sure everyone understands his or her role and security procedures.

Pre-event publicity for upcoming events should be reviewed in light of security. Potential gains in audience numbers must be weighed against the security concerns created by "going public."

For special events where tickets are inappropriate, you may choose to use a guest list or a sign-in book. Regardless of what you choose to use, no one should enter your facility without being greeted and observed. An usher will usually function in that role.

Other sections in this manual deal with the following related and important topics:

- Suspicious people,
- Unwarranted interest in your facility,
- Suspicious objects,
- Suspicious vehicles

## Elements of Security for Events

Event security rests on the simple principle of *excluding* unwanted persons and *including* welcome persons. This principle is complicated by the fact that one wants to make sure that those who are to be included are efficiently processed through security and those people feel warmly welcomed and not overly inconvenienced.

At the same time, those who are to be excluded need to be stopped before entering the premises.

- Failure to exclude someone who should be excluded is considerably more dangerous than failure to include someone who should be included. The former is a life and safety issue, the latter a constituent relations issue.
- In a manner that ensures the safety of persons who are in the vicinity of the person being excluded.
- In a manner that will cause the least disturbance and distraction for security personnel.
- In a manner consistent with local, state and federal law pertaining to discrimination and public accommodations.

**Steps for securing an event include**

- ✓ Assessing Risk
- ✓ Establishing a Perimeter
- ✓ Maintaining a Screening Center
- ✓ Keeping Vigilance High

## Assessing Risk

A number of elements go into any risk assessment; however, three stand out:

1. the existence of prior threats or incidents,
2. the extent to which the event is open to the public, and
3. the extent to which the event is publicized.

**Note:** There is no magic formula to determine what risk an institution has or does not have. The reality is that an event manager should try to make a series of educated guesses, in light of all the facts and circumstances known to him or her, in the hopes of thwarting an attack and mitigating damage.

## Who Is Invited

Typically, an event which is open to the public will have a higher risk profile than an event which is limited to members only. Very large institutions that publicize events to their members face a similar risk to an open, public event.

It may be helpful to think about events in the following three categories:

**Private events** are those events to which specific people are invited from a mailing list developed by your organization personnel and who are known to your organization.

**Public events** are those events that any person who purchases a ticket or shows up can attend.

**Limited access events** are any events that are *neither* strictly public nor strictly private. Examples include: events which require tickets to be purchased by check or credit card from a central location ahead of time, or events where someone else controls the invite list.

## Publicity

The next issue is whether the event should be publicized or not. An institution might face a lower risk if an event is known only to its members than if the event is publicized in a local newspaper. Larger, higher profile institutions logically face higher risks, though this is not a "hard and fast" rule as larger institutions usually possess greater resources to draw upon.

It may be helpful to think about publicity in the following ways:

- An event that is *not publicized* is one in which no public statement whatsoever (either through press release or news story) is released or published about an event.
- An event can have *controlled publicity* when the event is publicized but where *one* of the following *three* details is missing from *all* public statements and articles about the event:
    - Specific time
    - Specific date
    - Specific location

(Some institutions, for security reasons, will require participants to call for information and require the caller to identify himself/herself. This is what we mean by *controlled publicity*.)

- An event is *publicized* if it has any publicity that exceeds these two rules, whether accidental or not.

### Prior Threats and Hate Activity

Finally, it is worth discussing with your local police department and Anti-Defamation League Regional Office the nature and extent of prior threats and hate activity at Jewish institutions (locally, regionally, nationally and internationally).

In our view, the presence of prior threats or hate activity will increase the security profile of an event.

*It is critical to understand that individual institutions' situations vary*.

#### Important Note: How High a Profile Is the Event for Your Organization?

An organization running a high-profile event (Israel Day Fair), dealing with controversial issues (politics), having high-profile participants (a senator) and/or operating in a high-profile environment (e.g., during a time of raised anti-Semitism) should recognize that their risk may be higher. Institutions may wish to consider providing the highest level of security possible for any event that is publicized and/or open to the public.

## A Word on Publicity

As the grid above demonstrated, publicity is an integral part of the security equation of an event. ADL makes no recommendation about whether to publicize any given event, but we urge you to understand that the more publicity an event receives, the more likely it is to attract the attention of those who may wish you or your facility harm. When you make the decision to publicize an event, it is critical that you increase the strength of your event security.

In the end, consider:

- Is the benefit of increased exposure of an event worth the cost of having a greater risk and thus needing increased security?
- Is the benefit of higher attendance worth the cost of having a greater risk and thus needing increased security?

You may answer yes to these questions, but you may also determine that the marginal cost of having half a dozen new attendees is not worth the cost of increased security.

## Establishing a Perimeter

**The basic element of event security involves establishing a security perimeter.** Outside of the perimeter, wanted and unwanted persons mingle; inside the perimeter, only welcome persons are permitted. Your first task, then, is to identify the area you want to protect (e.g., an anteroom and ballroom, a social hall, a gymnasium, an entire building). In identifying perimeters you may wish to consider:

- The bigger the perimeter, the harder it is to secure — it takes more eyes to watch a larger perimeter than a smaller one.
- Is there a place at the perimeter to set up a screening area? If not, you may need to expand or contract your perimeter as necessary.
- Is the perimeter wide enough to prevent damage to interior spaces or persons from an attack on the outside (e.g., if an explosive device goes off outside your perimeter)? Keep in mind — you must balance the risk of attack against your ability and resources to protect and patrol the area secured.

**Consider:**

If you have a high profile, controversial event, for instance, you might consider the possibility that an explosive device left outside your event could cause serious damage inside and thus you may wish a wider perimeter.

Planners of a lower profile event in a low risk area may choose to be less concerned about that possibility.

- Perimeters do not need to make use of existing structures: you can set up an artificial perimeter to help by, e.g., using a rope line, tables or chairs organized to control traffic flow.

Once you have identified your perimeter, you should identify every way in and out of that perimeter. Include:

- Main entrance
- Emergency exits
- Kitchen doors
- Secondary doorways and entrances
- Windows
- Your security screening area

You will want to be able to secure the area so that anyone who wants to enter must go through your security screening center or is screened at a secondary screening area. Considerations include:

- Every possible way in must be *locked, guarded, and alarmed*. Remember, you must do this consistently with the fire code.

- Someone should be in charge of maintaining the perimeter and of supervising those who are assigned the task of patrolling the perimeter, guarding doors, windows, etc.
- Maintaining security when those responsible for the perimeter are distracted from their duties. For example, can your security officers be distracted by:
    - A patron voicing a complaint that distracts the security officer (e.g. about being denied access for want of a ticket). One solution: assign a non-officer troubleshooter, typically someone familiar with the people who are invited to an event, to assist at check-in and to whom a security officer can send those with issues or complaint.
    - The event they are supposed to be guarding (for example, will a notable speaker or intriguing performance have all of your security officers looking stageward not outward?). One solution: training and supervision.
    - Other responsibilities, such as being required to leave a post to assist in a medical emergency (for example, if someone falls ill, will your entire security staff be off of their posts?). One solution: have a medical emergency plan in place.

Once your perimeter is established, it is wise to clear the area inside of the perimeter and inspect the entire space, looking for anything — a device, a person — that may have been hidden before you established your perimeter. This would be, for example, when you let an explosives-detection dog sweep the area. Make notes of what is there that might later cause suspicion. Once the perimeter is swept, *only* those cleared through your screening center should be permitted inside.

## Maintaining a Screening Center

Your screening location should be designated as a location when people are cleared to enter your perimeter. It may be the place where a ticket is checked, a guest list consulted, where metal detectors are deployed — whatever you determine is necessary for your event. Your local police department can be of assistance in making this decision. At the very least, everyone should be visually inspected for suspicious characteristics and behaviors.

A few considerations:

- Entrance credentials — any ID that permits one to enter an event (e.g., table cards, event ID cards, etc.) — that are handed out at the check-in center should be distributed by staff, not left alone on a table for collection. We caution against having unstaffed name tag tables.

- It is important to secure or guard entrance credentials from theft. We also suggest that where name tags are displayed on a table, for ease of the staff checking people in, someone be assigned the job of ensuring that no one steals entrance credentials.
- For entrance credentials that are used to facilitate reentry to an event, consider collecting those credentials from people who will not be returning to the event. Your security will be compromised if someone can use a badge that he/she retrieved from a trashcan outside of the event. This is especially true of special credentials, such as press credentials.

Your security staff should:

- Ensure the perimeter remains intact
- Query anyone who is without a displayed entrance credential
- Look for unattended bags and packages

Security concerns for special events, parties, *simchas* may include the following.

- Assign ushers who can maintain a watchful eye and who understand that their job includes security.
- Not publish the name of a child or couple in any public newspaper or on the sign in the entranceway or on the street.
- Do a security sweep — a walk-through — before the event, no matter how low profile.
- Gifts set down become unattended packages: they should be kept on a special table and supervised.

# Guidelines for Hiring a Security Contractor[9]

Once a decision is made that your institution has short- or long-term security needs, it should be determined whether limited or complex security requirements are necessary. ADL strongly recommends that each institution undertake security as a long-term, ongoing process. Depending on the nature and complexity of the institution, an assessment by security professionals might be required.

## Short-Term Work

During holidays or special events where security officers may be required on a short-term basis, institutions should obtain competitive bids as soon as possible. It is essential to check with local law enforcement and other community agencies for recommendations. It is essential the institution clearly define the security contractor's scope of work. All of the following criteria should be met:

- A concise statement describing the security tasks to be performed, including the number of days and hours that security is needed. This information should be clearly outlined with the security contractor before security staff is assigned to the site.
- A detailed set of general and particular special instructions. The importance of these instructions cannot be overstated. The institution should not rely on the security contractor to provide them. These instructions should be discussed with and agreed upon between the decision-makers of the institution and the security firm. Contractors are to provide supplemental instructions to their personnel.
- Assignment of one person who will be the security officer's contact and will greet the security officer throughout the assignment. This liaison will greet the security officer upon arrival to ensure that the security officer understands his/her role, and among other requirements, has a neat appearance and proper attitude.

## Interactions with Security Officers

First impressions are important in determining how the security officer will perform. It is important to remember that the security officer is present to deter and detect unusual or suspicious activity as well as to safeguard property and people. The following are key points that the institution's contact person should discuss with the security officer:

- Requirements of the assignment.
- Purpose of security during the prescribed times.

[9] Prepared by the San Diego Regional Office's Inter-Agency Security and Safety Committee.

- The security officer will be assessed during the shift for alertness.
- Rules of conduct that enhance effectiveness. For example, no smoking, practical joking, fraternizing, etc.
- The scope of work should be explained and written concise expectations presented as soon as the security officer arrives (keeping a copy for yourself):
- Institutional contact and how to immediately reach him/her.
- Layout of the facility.
- Facility security and/or fire regulations.
- Any vulnerable areas.
- Locations of telephones, fire-fighting equipment, fire alarms, emergency exits, etc.
- Location of stairways and doors.
- Clear operational guidelines to be used in the event of an emergency (fire, suspicious package, bomb threat, etc.).

## Criteria for Security Contractor Selection

As soon as the need for a security firm has been determined on an immediate or long-term basis, a security contractor should be selected. Selecting a company that has valid, current state licenses is essential. You should be certain that a company is reliable and in good standing.

All of the following criteria should be met:

- Adequate and current insurance
- Track record/reputation
- Proposal characteristics
- References
- Training
- Equipment
- Costs
- Contract
- Management
- Security officers' qualifications

## Insurance

After you have established that a security contractor is duly licensed, scrutinize the insurance coverage the security contractor provides. Every state licenses and keeps records on security firms. As such, it is essential to hire a company that has a valid, current state license, and to determine the reputation of the company by investigating any history of complaints reported against it to the state licensing authority. The following insurance criteria should be met prior to hiring a security contractor:

- The contractor provides and maintains adequate insurance coverage for your situation.
- Your risk manager (insurance agent) approves of the contractor's coverage.
- Contractor's Broad Form General Liability Insurance covers a minimum of $1 million per incident and $3 million total. The higher the coverage the better. Determine whether the contractor has fidelity bonding and other coverage.
- The contractor's Workers Compensation Insurance is at statutory minimums.
- The contractor should have adequate Automobile Liability Insurance coverage for all vehicles used.
- Security contractor's insurance covers sexual harassment through their Professional Liability coverage.
- Liability coverage for special equipment provided (golf carts, computer equipment, watch clocks, etc.).
- Contractor's insurance carriers name your organization as "Additional Insured" on their liability insurance policies (or at least, obtain certificates of insurance for the contractor). If so, is there an extra charge for this?
- Your insurance advisor does not object to any of the policy "Exclusions."
- Ask for EMR (Employment Modification Rate) for the last three years. The lower the EMR, the better the contractor's safety performance.

**These criteria are important in determining whether a security contractor's insurance coverage is sufficient to meet your needs. A security contractor must both provide security and be properly insured.**

## Reputation

A security contractor's reputation should be examined to ensure that the company has maintained a trustworthy and dependable reputation. To determine the quality of past work, ascertain whether there has been a recent history of valid or successful lawsuits or complaints to state agencies against the contractor filed by clients or employees. This can be learned at your local courthouse or through a local attorney. Consider three main factors when researching a company's history: negligence, workers compensation claims and experience and management.

### Negligence

Determining possible history involving negligence by the contractor is important. Request "Loss Experience" or "Loss Runs" reports from the contractor in order to review its liability insurance claims history. Inquire of the contractor directly whether the company has ever been involved in any lawsuits and whether there has been any legal incident involving their employees while on a client's property during the last 10 years.

Your lawyer or insurance broker can explain the report and advise you on the significance of each case and report.

### Workers Compensation Claims

Review the listing of worker compensation claims to determine the possibility of patterns of carelessness or inadequate employee safety practices. This report is available from the security contractor and your insurance agent can advise you of the significance of each claim. Again, ask for EMR (Employment Modification Rate) for the last three years (the lower the EMR, the better the contractor's safety performance).

### Experience and Management

First and foremost, it is important to recognize that you are hiring the security officer service management team because, typically, the pool of security officers is the same for all companies. Inquire as to the number of years of service in the security industry of the contractor's president, regional manager and operations management.

Although not essential, the security contractor should have recently provided security service to an institution similar to yours.

## Proposal Characteristics

Carefully analyze the proposal submitted by the security agency. The proposal should address the specific security needs at your site and demonstrate that the security contractor has

carefully reviewed and considered your needs. The following are key points that the security contractor should enumerate in a proposal for your institution.

## Training and Qualifications

The proposal should set the minimum qualification as follows: describe the security-related education, training levels, and experience of personnel to be assigned at your institution. Security contractors that provide additional education and training to their staffs are preferable.

## Staffing

Staffing may be regular, rotating or temporary and it is important to know beforehand which personnel you will be dealing with. **A permanent staff assignment is always best if it can be obtained.** However, security contractors often have difficulty maintaining regular staff as a result of odd shifts, frequently consisting of less than eight hours. You should research the security contractor's history of staff stability and be wary of excessive turnover or poor relationships with employees. The contractor should also obtain your approval before transferring (or replacing) personnel from your site. It is important to assure that the contractor's needs at other sites should not take precedence over security needs at your site.

## Description of Supervision

Does the proposal describe the exact nature of supervision to be provided? Contractors should be willing to explain clearly how they will monitor and control the quality of security services.

## Documentation

In selecting the best quality contractor, the proposal should describe the type and frequency of reports and documentation (daily officer activity logs, incident reports, crime reports, officer time sheets, other special reports, etc.). Consistent and thorough written communication is an important output of contract security services and is an important management control mechanism you have over security services and costs.

## Instructions to Security Officer

Carefully analyze whether the proposal includes sample Post Orders or Standard Operating Procedures Manual. This document describes all aspects of job performance at your site including security officer grooming and decorum, sets the standard of security services, and provides the basis of guard discipline. Ultimately, this document becomes the main basis of legal defense in the event of litigation. The contractor should provide a document that is comprehensive and clear both to you and the security officers.

### Emergency Procedures

The contractor's proposal should describe how its security officers will function under various emergency conditions. The proposal should demonstrate an understanding and coherent approach to a wide variety of nonstandard, unusual or crisis situations.

### Equipment Issues

If the security officer is expected to patrol your institution when it is closed (holidays, overnight, etc.), he/she should be equipped with a cell phone enabling contact with emergency services if needed. It is important for you to ask what other equipment is standard issue and/or the security officer is certified to use. For example, will the security officer carry a baton, pepper spray, handcuffs, etc.?

## References

References help identify quality and reputable security contractors. Client references give invaluable insight as to the reliability and performance of a security contractor and highlight areas of possible improvement. To secure the most qualified and experienced security firm, use references that:

- Clients verify a contractor's history of relevant experience.
- Past clients' references verify a contractor's history of responsiveness.
- References indicate contractor's employee turnover rate is lower than or equal to that of industry norms.

## Costs

Prospective security contractors should address the following issues:

- How frequently will contractor bill for services rendered? Weekly? Biweekly? Other? Is this convenient for you?
- Will it be a flat monthly rate, a uniform hourly rate for all employees or a unique hourly rate for each individual employee? Generally, paying a unique hourly rate for each security officer provides clients with the most economical service.
- Contractor discloses wages to be paid to security officers assigned to your site. A good contractor should be willing to discuss openly all cost drivers and the fee or profit margins it expects to earn for the services to be provided.
- Contractor's periodic invoices list wages and bill rates for each security officer. Invoice detail provides a good audit trail and shows contractor professionalism.
- How will security officer pay increases be handled? Inadequate or stagnant wages are a frequent cause of staff turnover. Wage increases should be proposed in advance by the contractor, based on officer incentive and merit, reflected logically

in billing rate adjustment and mutually agreed upon by the contractor and client before implementation.

- Will any additional charges be made for uniforms, equipment, supplies, etc.? Again, these should be proposed, justified, logical and mutually agreed upon.
- Is the total estimated average monthly cost within your budget? Your monthly security officer budget can be calculated by multiplying the hourly wage rate.

## Contract

The security contract defines the rights and responsibilities between you and your contractor and ensures that the contractor will meet your needs. There are numerous questions and criteria that a security contract should specifically address in order to ensure that the security firm is responsible and dependable. These serve as guidelines to refer to and are listed below:

- Does the contractor indemnify you for all security-related liability for which the contractor is responsible? In cases where partial liability is determined by a court of law, does the agreement clearly specify how such indemnifications shall be applied? You should discuss client indemnification of the contractor.
- At contract time will there be a price increase? How much? Why?
- Do you retain the right to terminate the agreement at any time and for any reason? Is this right mutual?
- Is the amount of notice required for contract termination — by the contractor or client — reasonable? Thirty days is the standard.
- Is the agreement sufficiently flexible to meet your needs?
- Does it assure fairness to the contractor and adequate control to the client?
- Can you replace a security officer if necessary?

## Management

You and the security contractor must share an understanding of the reasons for entering into the contract. As such, discussion issues should include the following:

- Discuss your desires with the security company management.
- Discuss terms of supervision with the contractor, field and management staff. The security personnel know, understand, and comply with your site's written policy manual. If a security officer performs below par, it is important to know that the individual will be counseled, disciplined and replaced by the contractor as needed.

- Once the security officers are in place, you will need to monitor them to ensure that they meet high professional standards, project a professional and alert demeanor and respond effectively to security-related concerns. It should be required that all written materials from the security officer (logs, reports, etc.) be clear, complete and useable. You should receive a copy of every report filed by your security officer.

## Deciding What Kind of Security Should Be Hired

It is important to know that hiring a security contractor, whether limited or extensive, armed or unarmed, is a serious business and not to be taken lightly. Different kinds of security officers are appropriate for different situations. One important issue is whether you would like security at your site to be provided by a uniformed or plainclothes security officer.

- The main goal for hiring a uniformed security officer is deterrence.
- The main goal for hiring a plainclothes security officer is apprehension.

After deciding what kind of security to hire, you must determine whether the security officer should be *armed* or *unarmed*. There are many costs and benefits to be considered when choosing an armed versus unarmed security officer.

The following should help you analyze the issue and determine what is in the best interest of your institution.

### Armed Security Officers

**It is important to determine if hiring armed security officers meets your institution's expectations for security.**

- **Realize that armed officers may utilize deadly force.**
- Determine the training qualifications the security officers have with firearms.
- Determine the contractor's policy on the use of weapons with regard to deadly force.
- Keep in mind moral questions when hiring an armed security officer. You should determine whether the members of your institution will accept an armed officer on the premises. Please note that special care should be taken if your institution serves many young people. Schools should be particularly concerned with the message an armed security officer conveys to students, parents and staff.

- Consider the cost effectiveness of an armed security officer. They are much more expensive than unarmed security, due to licensing and training requirements.
- Decide whether the presence of a weapon may escalate the possible use of force and violence which otherwise may not occur.
- Insurance may be adversely affected by the presence of an armed security officer.

### Unarmed Security Officers

- Use of deadly force is neither desired nor required.
- Unarmed security officers often provide the same deterrent as armed officers without the risk of deadly force.
- The protection afforded by unarmed officers is less expensive and may incur less liability and insurance.

## Checklist for Security Contractor Selection

As previously mentioned, when the need for a security firm has been determined on a short- or long-term basis, a security contractor should be selected. The following checklist has been developed to assist you in this process:

**Institution Name** _____

**Security Contractor Name** _____

| | Requested | Received | Accepted |
|---|---|---|---|
| Insurance | | | |
| Reputation | | | |
| Negligence | | | |
| Workers Compensation Claims | | | |
| Experience | | | |
| Proposal | | | |
| References | | | |
| Costs | | | |
| Contract | | | |
| Management | | | |
| Security Officers | | | |

# Suicide Bombers

This is, without question, the most difficult topic to consider and take action against.

Statistics indicate that the chance of a suicide bomber attacking your institution is remote. Such an event is obviously extremely dangerous and potentially deadly. While the risk of such an occurrence is very small, the possibility requires an institution give the issue some consideration and thought.

**A word of caution: no security manual can adequately provide a response plan to this phenomena.** What we attempt to do here is raise the issue, providing some insight into the phenomenon, so that you and your key staff can have a serious discussion of — and effective role-playing about — possible responses. It goes without saying that such responses will involve very hard choices made in a very compressed time period with serious repercussions.

The possibility of a suicide bomber is perhaps one of the most horrible security issues you will be called upon to consider. **THERE ARE NO EASY, CANNED ANSWERS TO THIS THREAT.**

## Role-Playing

> It may be very useful to utilize a professional in developing role scenarios and analyzing lessons learned.

We strongly recommend that members of your security committee, the board of directors and your "front line" personnel — greeters, ushers, hired security officers or their managers and/or others — role-play as a team possible threat scenarios and responses. To do this, you may wish to determine whether any member of your institution has experience in this field. Otherwise, you and a small group should develop scenarios involving the approach of a suicide bomber, his/her attempt to gain entrance and the possibility that he/she may actually gain entrance to your facility and detonate. It is important to alter the nature of the scenarios and carefully analyze lessons learned. For instance, if role-playing leads you to try to engage the suspicious person in conversation while someone else dials 911, you need to determine (a) who will dial 911 or contact emergency personnel, and (b) what you will say to the bomber to try to engage him or her.

## Possible Indicators of a Suicide Bomber

There is no commonly accepted or developed profile of a suicide bomber. Studies indicate that the only characteristic accepted by experts is that the overwhelming majority are prepared to die in the service of their cause.

Suspicious people may often be identified by their behavior. While no one behavior is proof that someone is planning to carry out an attack (many of the following behavioral indicators are perfectly consistent with innocent behavior) and while no list could ever be complete, these factors can help you assess whether someone poses such a threat.

## Behavioral Factors to Consider

- Nervousness, nervous glancing or other signs of mental discomfort/being ill at ease. This may include sweating, "tunnel vision" (staring forward inappropriately) and repeated inappropriate prayer (e.g., outside the facility) or muttering. This may also include repeated entrances and exits from the building or facility.
- Inappropriate, oversized and/or loose-fitting clothes (e.g., a heavy overcoat on a warm day).
- Keeping hands in pockets or cupping hands (as if holding a triggering device).
- Constantly favoring one side or one area of the body as if wearing something unusual/uncomfortable (e.g., a holster or a bomb belt or vest). Pay attention to a person constantly adjusting waistbands, ankles, or other clothing. Projected angles under clothing may also be indicative of a firearm, e.g., at the waist or the ankle. Suicide bombers have been known to repeatedly pat themselves to verify that the bomb vest or belt is still attached.
- Carrying packages.
- Security personnel should be told to observe people, when possible, as they exit their cars. This can be done by watching how they adjust clothing and how they approach the building, looking for signs that a person might be carrying a weapon, etc.

Again, many of these, especially the last, are often consistent with perfectly innocent explanations.

**The most important thing is to be observant.** For example, Israelis have become aware that some suicide bombers shaved off their beards prior to committing their acts, thus leaving unusual facial tan lines. (In Israel, the majority of bombers have been males, 18–27.) Some also anointed themselves with scented oil, which may be obvious to someone in their vicinity.

## Responding to a Perceived Threat

While no one factor is a certain indicator of a problem, once a potential threat is identified, ushers and security personnel have three options: do nothing, investigate before deciding whether to take emergency steps or immediately take emergency steps. **This is a decision only you can make in light of the circumstances, your personal comfort level and safety considerations.**

You must, at all times, be aware of the threat to worshipers, students or others if the individual about whom you are concerned gains access into your facility.

If you choose to investigate, one technique is to greet the person in a friendly fashion, asking, "Can I be of assistance?" Evasive or unusual answers may trigger your emergency procedures. Excuse yourself and initiate your procedures, perhaps by using a predetermined code word with your colleagues. If you believe that a person poses a threat, we urge you to try to prevent entry to the facility.

If you choose to call 911, make sure the dispatcher understands the emergency nature of the call and the need for law enforcement to respond without sirens.

***If you remain suspicious, trust your instincts. Even if the person leaves immediately, call the police.***

## Disturbed Individuals

One somewhat related problem is dealing with what might appear to be a disturbed individual. Only you can make a decision on how to proceed in light of given facts and circumstances.

This is a tough call. We suggest you exclude any individual who you think poses a security risk. However, if you choose to admit the person to the facility pending assistance (e.g., arrival of police) it is important that the person be monitored (for example, invite the person to sit in an aisle seat). Assign an usher or employee to monitor the location of the individual and his or her actions to determine whether any additional, immediate action is necessary.

# A Brief Look at Weapons of Mass Destruction (WMD)

This chapter is intended to provide general information in an effort to enhance your knowledge and to assist in efforts to recognize potential WMD-related threats or incidents. It is adapted from a fact sheet provided by the Federal Bureau of Investigation. Other government sources, such as the Federal Emergency Management Agency, can provide additional information about how to respond to a WMD incident. **This information is not exhaustive.**

## Of Critical Importance

WMDs are extremely hard to manufacture. They are also extremely difficult to deliver effectively. Finally, most so-called weapons of mass destruction will have a limited effectiveness range. Thus, your risk from WMDs is likely to be minimal. However, it is still important to understand WMDs and be able to prevent and react to their use.

Chemical, biological and radiological material can be dispersed in the air we breathe, the water we drink, or on surfaces we physically contact. Dispersion methods could include placing an open container in a heavily used area, using conventional garden or commercial spray devices or detonating an improvised explosive device to disseminate chemical, biological or radiological material.

Chemical incidents are characterized by the rapid onset of medical symptoms (minutes to hours) and easily observed signatures (colored residue, dead foliage, pungent odor and dead insect and animal life). In the case of a biological or radiological incident, the onset of symptoms may take days to weeks and there are typically few characteristic signatures.

Your alertness to the following signs might assist law enforcement and emergency responders in evaluating a potential WMD threat:

- Unusual packages or containers, especially those found in unlikely or sensitive locations, such as near HVAC or air-intake systems.
- Unusual powders or liquids/droplets/mists/clouds, especially those found near air-intake/HVAC systems.
- Indications of tampering in targeted areas/equipment (e.g., locked ventilation/HVAC systems, stocks of food, water supply).

- Reports of suspicious person(s) or activities, especially those involving sensitive locations within or around a building.
- Surveillance of targeted areas, including but not limited to hotels, entertainment venues, subway systems, aircraft, water sources, office buildings, apartment buildings. Theft of chemical products/equipment.
- Dead animals, birds, fish or insects.
- Unexplained/unusual odors. Smells may range from fruity/flowery to sharp/pungent, garlic/horseradish-like, bitter almonds, peach kernels, and newly mown grass/hay (realizing that some of these smells have perfectly innocent explanations).
- Unusual/unscheduled spraying or discovery of spray devices or bottles.

## Protective Measures

- Maintain a heightened sense of awareness.
- Place an increased emphasis on the security of immediate surroundings.
- Conduct periodic inspections of building facilities and HVAC systems for potential indicators/irregularities.
- Review emergency operations and evacuation plans/procedures for all locations/organizations to ensure that plans are up-to-date.
- Promptly report suspicious activities to appropriate law enforcement authorities.

## Emergency Procedures—Potential Threat Identified and Confirmed

- Maintain a safe distance and/or evacuate area (if outside, move to upwind location; if inside, keep outside doors and windows closed).
- Call your local 911 (law enforcement and public safety personnel) after reaching safe area.
- Do not handle or disturb suspicious objects.
- Remove possibly contaminated external clothing (including hats, shoes and gloves).
- Follow emergency operations plans and/or instructions from emergency response personnel.

**Note:** In an effort to prevent spreading contamination and to ensure appropriate decontamination and medical treatment, after moving to safety, do not leave until instructed to do so by law enforcement.

# 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:

- Evacuation after a called-in bomb threat
- Denial of entry to suspicious persons
- 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.

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 your response 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:

- Security threats (e.g., bomb threats)
- Allegations that may expose the institution to legal liability or embarrassment
- 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
- Any inconsistency between expected and actual bank balances
- Requests for information that is inappropriate (i.e., a request by an unknown person for an employee's home address)
- 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)
- Requests for donor information
- Attempts to improperly access computer systems and/or "hack" an institution's Web site
- All other contacts that concern the employee
- 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. He/She should:

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

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

    - 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")

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

## 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 example, is your staff able to deal with the following (all of which are covered in this manual):

- Explosive Threats
- Armed intruders in schools
- Computer crime targeting your institution
- Evacuation procedures

## The Crisis Management Continuum: Crisis Management

### The psychology of crisis decision making

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

**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.

**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.

### 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 his/her crisis manager identify those members of the crisis team that will staff this crisis and then pull that team together. In the meantime, he/she should focus his/her attention on managing the crisis.

A crisis team in action should have several features:

- **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.

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

- **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.** 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.

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.

Have the means to communicate — and be communicated with.

- Know telephone numbers, email addresses, and other ways of contacting key managers, constituents and media contacts. Make sure that employees know how to reach the command center to report information.
- 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") or wireless communication and applications 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:

- 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.
- This spokesperson should be the sole contact point for the media, constituents and anyone else who needs information from the institution.
- Depending on the nature of the incident, especially if it involves children, the spokesperson might direct constituents to a further contact point.
- Information should be clear, factual, non-emotional and consistent with law enforcement requirements.
- 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.
- 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.")
- 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.
- 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.
- Practice the statement before presenting to the media.

**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.**

# Post-Incident Procedures

Once you have handled basic life-safety and emergency response procedures — in other words, as soon as you have established your initial response to a situation — your next task is to appropriately handle communication, evidence, disaster recovery and post-incident reviews.

## Command, Control, and Communication

As we have explained elsewhere in this manual, it is critical to establish chains of command, control and communication. Besides preventing what may be counterproductive or, worse, deadly confusion during an incident, it will also help you manage those *outside* of the immediate incident, including those who need or want information, such as the media and parents.

- Designate a single spokesperson for the institution. If it is necessary to have more than one, it is essential that they be carefully coordinated.
- This spokesperson should be the sole contact point for the media, constituents and anyone else who needs information from the institution.
- Depending on the nature of the incident, especially if it involves children, the spokesperson might direct constituents to a further contact point.
- Information should be clear, factual, non-emotional and consistent with law enforcement requirements.
- 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.
- 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.
- In order to not 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.
- When speaking to the media, be clear, direct and honest. Speak in short, declarative sentences. ("The facility will remain closed for the next two days.")

- 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.
- 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 refrain from mentioning certain facts so as not to taint a jury pool, to help them keep certain facts quiet so that they may determine if a subsequent incident is a copy-cat or not, and/or to ensure that an ongoing investigation is not otherwise damaged.
- 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.
- Your ADL Regional Office is available to help you deal with media, for example, by helping you craft a message or work with you on delivering it.

### When Communicating to Constituents

Be clear, direct and honest. If possible, be reassuring.
Remember that you may be dealing with people who are very anxious and afraid.

## Evidence

Consistent with your safety, it is absolutely critical that you seek to preserve evidence of any attack on your institution. This includes the following.

- Do not erase or paint over graffiti until the police say you may do so. While the temptation to erase graffiti is a strong one, it is very important that the police are able to examine the graffiti firsthand and get evidence from it.
- Consistent with your safety, take a picture of whatever is your cause of concern.
- Once you have removed yourself to a safe location, try to record, in writing, every element of the event or incident that you can remember. Write down a description of every mark, note, word or item on a suspicious package or note the license, color, make, and model of a suspicious vehicle. Fill out the bomb threat call sheets when a threat comes in; we urge you to similarly record every detail, no matter how small, when any other type of incident occurs. Remember: you and other staff members may have differing accounts based on perspective, memory and point of view.

- Do not handle evidence (e.g., a rock thrown through a window). While sometimes it is advisable to place a suspicious mailed package into a ventilated room, in no other circumstances should you handle a device or other item of concern. See "Explosive Threat Response Planning".

## Disaster Recovery

Disaster recovery may be a part of your post-incident work. Recovery can be made easier if some preparation is done beforehand.

### Consider

- Having off-site, current back-ups of critical data, vendor lists, employee, constituent and donor contact lists and other mission-critical information. This can be accomplished with a physical local back-up, such as a portable hard drive which is kept in a safe place when not in use or a web/cloud based back-up service.
- Conducting an insurance review to ensure that your insurance is adequate to your needs. Ensure that insurance records are kept with back-up information.
- Discuss with your attorney the legal aspects of recovery, including discussing whether someone has the legal authority to take emergency steps on behalf of your institution.
- You may also wish to have worked out plans ahead of time for relocation of students, patients, campers, etc.
- Anything else that, if destroyed, would cause your institution to cease running. You may wish to factor in any service agreements you have and whether they provide for adequate post-disaster service provision and recovery.

## Post-Incident Reviews

Once an incident is over and the recovery operation is in place, it is critical to review the events as soon as possible.

There are four key steps to the post-incident review. In particular, if there is a threat of civil or criminal litigation, you may wish to discuss the following steps with your attorney before proceeding.

1. Review the entire event, minute by minute, in an effort to determine what happened and when. Derive from this activity an assessment of what worked and what did not work. This is not the time to assign blame, but rather to understand what lessons you could learn.

2. Review your threat assessment in light of this incident and the new circumstances your institution may face. For instance, an arson attack may both reveal a previously uncontemplated threat *and* place the institution in the spotlight, creating an incentive for copycats.

3. Revise your security plan accordingly, ensuring that all discovered security needs are filled in.

4. Practice and drill on the new plan.

# Sample Quiz

The following are sample questions that institutions may use to help train their staff on security measures mentioned throughout the manual.

1) Who is responsible for security at your institution?
2) How does your institution maintain access control?
3) What behaviors are considered suspicious activity?
4) What are the characteristics of suspicious mail?
5) How should one respond if they come across a suspicious object?
6) How should one respond to a phoned-in explosive threat?
7) What are the options for responding to an active shooter situation?
8) What are the steps for responding to vandalism or graffiti?
9) Why should you not engage/debate protesters at your institution?
10) Who at your institution is responsible for responding to media inquiries?
11) What is the best response to a threatening e-mail?
12) Who should be contacted in the event that your institution's website is hacked?

# Appendix: Checklists

DENVER POLICE DEPARTMENT

## BOMB THREAT CALL CHECKLIST

# ASK:

**1. WHEN?** (WILL IT GO OFF)

**2. WHERE?** (IS IT LOCATED)

**3. WHAT?** (TYPE OF BOMB IS IT)

**4. WHAT?** (TYPE OF EXPLOSIVE IS IT)

**5. WHY?** (ARE YOU DOING THIS)

**6. WHO?** (ARE YOU)

# BOMB THREAT CALL CHECKLIST*

DATE _____ TIME OF CALL _____

CALL RECEIVED BY: _____ OFFICE: (  ) _____ EXT: _____

EXACT LANGUAGE OF THE THREAT: _____

_____

_____

VOICE ON PHONE (Check as applicable):

☐ MALE ☐ FEMALE ☐ ADULT ☐ CHILD ESTIMATED AGE _____

SPEECH: ☐ SLOW ☐ RAPID ☐ NORMAL ☐ EXCITED ☐ LOUD ☐ FOUL

☐ BROKEN ☐ SINCERE ☐ ACCENT ☐ INTOXICATED ☐ IMPEDIMENT

☐ SOFT/HIGH PITCHED ☐ DEEP ☐ CALM ☐ ANGRY ☐ RATIONAL

BACKGROUND NOISES: _____

_____

☐ MUSIC ☐ TALKING ☐ LAUGHING ☐ BARROOM ☐ TYPING MACHINES

☐ TRAFFIC ☐ AIRPLANES ☐ FACTORY ☐ TRAINS ☐ QUIET ☐ OTHER

NOTIFY: _____

SUPERVISORY OR COMMAND OFFICER

ADDITIONAL COMMENTS: _____

_____

_____

_____

_____

_____

_____

*MAKE A BOMB THREAT OFFENSE REPORT AND ATTACH THIS CHECKLIST

PD 199 (7/76) [Adapted]

Anti-Defamation League®

605 Third Avenue
New York, NY 10158-3560
www.adl.org