Protecting Your Religious and Communal Institutions

Used with permission.

INTRODUCTION

Members of our religious and communal institutions look to our institutions for a sense of community, comfort, and belonging. This is what we want for our communities. However, the unfortunate reality is that any institution may become a potential target for extremists, shattering this sense of comfort and safety. In order for us to do everything we can to protect our institutions and communities, we have a responsibility to create security plans and to make security a priority and part of the culture of our institutions.

The Anti-Defamation League (ADL) is a civil rights organization founded in 1913 to fight anti-Semitism and all forms of hate. ADL has been providing security guidance to Jewish institutions for decades. This document was created to share security best practices with other religious and communal institutions.

Security planning is a long-term process which involves consultation with, and training of, many members of your community. We urge you to use this document as a starting point for a conversation with selected members of your staff, leadership and a security professional who can assess your institution firsthand.[1]

While no guide can provide a security plan for each institution, there are some considerations all security planners must take into account. This guide is designed to help you think through some of these difficult issues and to begin the process of creating your own security plan.

A note: this guide is designed with many different types of institutions in mind. Although every item may not appear to be directly relevant to your institution, you may find that many of the items are still useful.

AN INTRODUCTION TO SECURITY PLANNING

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 communal institutions 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:

---

[1] **An important note.** This guide is intended to help institutions become aware of basic security considerations. It is not intended to provide comprehensive, institution- or event-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 the use, nonuse or misuse of this information. In addition, compliance with all life-safety codes, including fire codes, is critical.

1. Professionals and leadership should assess the risks to, and realities of, the institution when developing a security plan, and should seek 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. 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 your critical "eyes and ears"). When planning or participating in events, everyone—ranging from the Board President to the custodial staff — must ***think security***.

2. Community members have an important role in ensuring the safety of their communal institutions. Leadership must 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
    - Actively work to create a culture that is both secure and welcoming; and
    - Support the board and professionals as they make the difficult decision to create and implement an effective security plan.

Staff, leaders, and community members must be motivated and educated to understand the need to create and implement a security plan.

It is important to note that creating a plan, installing hardware and/or hiring additional staff are just the start 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, review of and updating your security plan are critical to your institution's security.

CREATING A SECURITY PLAN

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.

- ***Assessment***

  Identify Threats. First, you must assess the danger to your institution. Here are some tips on identifying potential threats:

  1. What does the news tell you about the current national and international climate?
  2. What do police tell you about the local climate?

3. What does the ADL Regional Office in your area say about extremist activity in your area?

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 them in your strategies. Note also that sometimes these things are related: the theft of a computer that contains membership lists and payment information can do great damage to an institution's reputation and members' safety.

Relationships with Law Enforcement. We urge you to recognize 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 who will be the first responders to an incident at your facility. The worst time to meet your local officers for the first time is during a crisis.

- ***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 event, lines of command, control, and communications are essential. Here are some considerations:

1. Identify a decision maker who will have the authority to act.
2. Ensure that decisions can be effectively communicated to those who need to know.
3. Plan contingencies in case a designated decision maker is unavailable during an emergency, whether out sick, on vacation, at lunch, or away from the office for a meeting.
4. Be able to ascertain who is in charge at any given point, including developing a succession list or chain of command in the event of an absence, even a temporary one.
5. Create a simple, user-friendly form to document threats coming to the institution, whether by phone, mail, or other means, containing checklist items identifying the threat and person making the threat, so staff can readily fill out and identify characteristics for law enforcement should an investigation be needed. Women's health clinics and at-risk facilities use this approach to document ongoing threats.

Suspicious Persons. Any security plan must include training and procedures for dealing with suspicious persons. In particular, staff should be aware of anyone paying unusual attention to, photographing, or loitering around your institution because such persons could be assessing vulnerabilities before launching an attack.

Explosives Planning. Planning should include creating and maintaining a bomb search plan and emergency evacuation plan. Some thoughts:

1. Create and maintain a bomb search plan and emergency evacuation plan.
2. Contact and include your local police department and/or bomb squad in your discussions. They will explain the actions for which a facility is responsible during a bomb emergency, including searching, and when they will respond. Many bomb squads will not come to a site until a suspicious item has been discovered. As many bomb squads do not allow individual organizations to contact them, communication with the bomb squad may need to go through the local police department. This is yet another reason to develop a relationship with the local police department.
3. Identify ways to notify and, if necessary, evacuate everyone in the facility during an emergency.
4. Designate a meeting point to ensure that everyone is safe and is out of your building or office.

Varied Use Plans. Create plans addressing varied building uses. School days and high-traffic events, such as community meetings, and days when the facility is not used create different security circumstances.

Business Recovery. Review business recovery plans, strategies, and all insurance policies. Business recovery plans may include off-site data storage, vendor and membership lists, and plans for emergency corporate governance policies.

- ***Implementation***

Implementing a security plan requires accountability, constant review and training, and relationship building.

Accountability:

1. Designate a staff member as security manager, accountable for implementing, reviewing, and constantly updating the security plan.
2. Make sure that everyone is trained to implement the plan, especially those who will be on the front lines and those who know the building best, the maintenance personnel.
3. Ensure that the security manager is a responsible, organized senior staff member, who will have enough time to fulfill security responsibilities, especially when first assuming the position. Often, the security manager has no security experience and may have a significant learning curve and time commitment. This person is responsible for continued training and updating the plan.

Plan Review. A security plan must be constantly reassessed and updated. A stale plan is no better than – and can be worse than – no plan at all.

Training Is Critical. Conduct community and staff training, drills, role playing, and regular refresher exercises. Drills and role-playing ensure that the plan is workable, up-to-date, and fresh in people's minds.

Build Relationships. At every stage of security planning, build relationships with the local emergency services.

1. Get to know local law enforcement, and get them to know the institution, *before* there is a problem.
2. If your facility has a gym, you may wish to invite local police officers to use the gym, to join members for a weekly religious service, holiday festivals, celebrations, special events, community meetings, or just to visit the building and become familiarized with the premises, personnel, and standard operations.

PHYSICAL SECURITY

Physical security starts with a basic premise: those who do not belong on the institution's property should be excluded from the institution. This occurs 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 by a locked door.
3. When those who do not belong are denied admission because they themselves decide that the institution is too difficult to enter, and thus, they do not even try.

There are a number of elements to physical security:

- ***Access control***

  Maintaining "access control" means that when the facility or office is open, no visitor, delivery, service person, or unknown individual is able to enter the facility without being directly or indirectly observed and approved. Some considerations:

  1. *Security desk*. Establish a protected security desk in the main lobby of each building or office with an open-access or open door policy. A sign-in/out logbook supervised by an employee who validates identification *prior* to allowing visitors to proceed into the building is highly advisable.
  2. *Monitor entrances*. Ideally, an institution or office should have a single entrance, monitored by a staff person and equipped with an intercom system for communicating with anyone who comes to the door. External barriers may also be considered. It is easier to prevent entrance into your building than to get someone to leave. An open door policy does not mean every door needs to be left open and unlocked.
  3. *Check credentials*. Before allowing individuals to enter institution property or offices, check that their identification papers or other credentials, including membership cards, are valid. Police and most utility employees carry identification cards and other documents. Three notes:

- Employees cannot always tell the difference between valid and forged documentation and credentials. Police and most utility employees carry such identification, but staff may not be able to accurately distinguish real and fake IDs.
- A uniform or equipment may readily be purchased, enabling an intruder to pretend that they have a legitimate reason to enter the facility.
- It is worth a few moments to contact the person's company or organization to determine the legitimacy of the person requesting admittance. Never be embarrassed to ask for more identification or to ask a person to wait until his/her identity is checked. Any individual who becomes agitated or angry at such a request should be considered of questionable legitimacy.

4. *Photo identification*. All employees should have identification cards, to immediately identify non-employees, and settle identity questions. Some thoughts:
   - All employees should be provided with and wear photo identification cards. Photo IDs enable individuals to immediately identify those who work in an institution and understand that they are part of their organization's security program.
   - Photo identification should not be issued without accompanying education about their care, procedures to follow if they are lost, and the manner in which employees should approach unknown individuals.
   - Using ID cards requires care. Cards should have clear photographs, along with the employees' names. Each institution must decide if their name should be placed on the card.
   - Employees should be instructed to wear their cards prominently while in the building and, for their own safety, kept from view when away from the building. There is no reason why any person on the street or on a train should be able to identify who someone is and where he or she works.
   - Lost cards should be reported immediately.
5. *Visitors*. At no time should visitors be allowed to roam freely through the property or office unescorted or without being observed. This is especially true for individuals who expect to work on the most sensitive systems such as burglar alarms, fire alarms, communication systems, or computers. Special diligence should be applied to those individuals when they visit the institution. For larger institutions, certain areas should be considered off-limits to all but authorized personnel.
6. *Open access facilities.* Community centers for youth and seniors, facilities with gymnasiums, and other institutions, desire to maintain open and free access. Allowing visitors free access to the facility does not mean they should be allowed to go anywhere, such as to restricted areas or office spaces. Visitors should perceive that institution personnel observe their presence and actions.
7. *Stay-behinds*. End-of-day locking procedures should include a visual examination of all areas of the institution to prevent "stay-behind" burglars.

- ***Key Control***

A key-control policy is essential to a sound security program. Failure to track those who have keys to specific locks or knowledge of alarm codes at all times defeats the purpose of a security system.

Institutions should bear in mind that disgruntled former employees or volunteers might subsequently break into the building.

Key Control considerations:

1. *Registry*. A central key control registry should be established for all keys and combinations. Employees and leadership should be required to sign for keys upon issuance and receipt. Key return should be part of ending service and exit interviews, if applicable.
2. *Issuance*. Supervisory approval should be required for 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 restricted number of employees and should be checked at least twice each year.
3. *Rekeying*. When key control is lost, rekeying an institution's locks may be worthwhile.
4. *Combination locks and codes*. Where combination locks and coded locks are used, combinations and codes should be changed at least every six months or when employees or leadership leave service. The combination should also be kept under strict management control.
5. *Special keys*. It is good policy to use locks with keys that cannot be duplicated without special key blanks.
6. *Key card readers*. Key card readers, while expensive, make key control and locking more effective and nearly automatic. Large institutions, or those with valuable assets, may find key cards worth the investment because they can control and track who comes and goes into specific rooms at any time.

- ***Locks***

Durable locks are essential to building and operational security. A professional locksmith should be consulted. While the suggestions offered in this section are detailed, every institution has unique local circumstances to be addressed. The following is intended as a starting point for discussions with an experienced locksmith who can assess an institution's circumstances and provide specific recommendations. Door locks should be chosen and installed to provide appropriate security levels for each location. Some considerations:

1. 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.
2. Dead-bolt locks are the most reliable and should seat at least an inch into the doorframe or lock-bolt receiver. Drop-bolt locks should be installed with the proper strike: wood frame, angle strike, metal frame, and flat strike.

3. Padlocks should be of high-grade material designed to withstand abuse and tampering.
4. Lock cylinders should be highly pick-resistant.
5. At all times, the door-locking system must meet applicable life safety and fire codes, to allow emergency exiting without impediment.
6. The jamb must be sufficiently strong, as a strong lock entering a weak jamb will fail.
7. 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.
8. Automatic closers. Doors that have air, hydraulic, or spring returns should be periodically tested to ensure that doors return to the fully closed or locked position.

Lock management. The institution's security manager should be responsible for the following:

1. Regularly inspect and report all damaged locks and ensure that they are repaired quickly.
2. Establish a chain of responsibility for all locks at doors and windows; ensure that locks are indeed locked, and report all failures to do so.
3. Ensure that keys are not left unattended.
4. Recommend installation of additional locks where necessary.
5. Add the locking key control program as part of the periodic security audit.
6. *Remember to survey all lock locations*. In addition to exterior locations into the facility, locks are present on interior doors, windows, offices, filing cabinets, and storage closets.

- ***Protective Devices, Alarms, and Technology***

Selection, specification, and installation of protective devices and security technology require professional advice. Begin by contacting local law enforcement and requesting help from the crime prevention, crime resistance, or burglary prevention officers who are specially trained and can offer expert guidance.

Protective devices, including intrusion detectors, fire detection systems, alarm systems, and cameras slaved to a closed-circuit TV (CCTV) system, can be an important, and costly, part of institutional security. CCTV coverage allows surveillance of exterior exits and interior corridors by a trained security officer at the central control console. However, even the most sophisticated and costly devices are limited by human factors, including failure to watch monitors carefully.

1. Many types of technology systems are available on the market for institutional applications. Selecting the appropriate system can be a challenge to the layperson. Institutional facility managers, members of the institution's building committee,

licensed architects and engineers, as well as reputable, and ideally, certified, security consultants can assist with selecting appropriate technology and protective devices. Ultimately, the facility manager or administrator must understand how to use and maintain the system and be sure that any technology performs the necessary tasks to secure the premises.

2. CCTV systems will be marginally effective if they are not properly maintained and monitored, or if those tasked with monitoring cameras are overworked, poorly trained, tired, or distracted. Most institutions are unlikely to have resources for continual monitoring. An alternative is a videotape or digital system. Video surveillance will fail when not properly used, or when no one is assigned to check, review, and change the tapes. Digital systems can store images on a computer console, rather than on racks of videocassettes, and can call up specific views and times on a computer screen when programmed.
3. Surveillance cameras should be placed at the institution's entrances, as a deterrent to potential intruders. Cameras can document criminal acts occurring on the property, which can later be used to identify and prosecute perpetrators. Although first costs are often expensive, in the long run, cameras are economical when compared to the costs of potential losses:
    - Use wide-angle lenses to survey entrances.
    - Use cameras with infrared illumination to enhance nighttime video.
    - Couple the camera with a time-lapse recorder for permanent recording.
    - Make sure the camera has a time and date recorder.
    - Compare the cost of color versus black and white, digital versus video.
    - Save video film for a minimum of one week.
    - Replace video film at least every six months.
    - Investigate digital capabilities.
4. Alarm systems, like locks, require professional guidance. Alarm systems are designed to alert an institution to an intrusion, and can materially benefit facility security. The size, location, and type of institution will determine the type of system required. Some thoughts:
    - Ensure that all alarm systems have emergency backup power sources.
    - Conceal the alarm control box and limit access to it.
    - Choose the system that best fits the need of the establishment.
    - Select a system with an electronic circuit delay of 30 seconds.
    - Ensure that the alarm can be heard throughout the property.
    - Contract with a central alarm monitoring company to monitor the alarm system.
    - Protect all wiring components and sirens from tampering.
    - Test the alarm system regularly to maintain effectiveness.
    - Apply alarm-warning stickers in windows, entrances, and exits.
    - Ensure that the alarm system meets local legal and code requirements.
    - Determine if the city or town prohibits directly dialing to police.
    - Educate staff and leadership about using the equipment and how the monitoring company will handle all alarms, including false alarms.
    - Consider adding panic buttons to the alarm system, to allow the alarm to be triggered from locations other than the main alarm panel. Consider panic

button placement in key offices used during off hours, and in locations where intruders may first be confronted, such as in reception areas.

- Special features might include emergency panic buttons and robbery signal circuits.
- Motion detectors or automatic sensors responding to sound or movement are excellent protective devices, used alone or in conjunction with the institution's lighting system. These detectors and sensors are economical and can be used inside or outside the building.
- Two effective, inexpensive solutions are alarms using magnetic contacts and trip wires. Alarms with motion, sound, or light detectors are more expensive, but are generally more dependable. The cost invested in a dependable alarm system is generally less than the cost of damages caused by an intruder to the institution.

- ***Doors***

When renovating, upgrading, or modifying existing facilities, or designing new facilities, a licensed architect and engineer should be consulted to design and specify appropriate, code-compliant windows, doors, screens, gates, skylights, and building construction materials, and to ensure that facility design meets applicable local life safety, building, and fire codes.

All exterior doors, main building doors, and lobby doors leading to common corridors should meet several important criteria.

1. Solid core, wood, or metal are acceptable, depending on code requirements.
2. Glass door panels or side panels should be reinforced with metal or steel mesh, or else replaced with shatterproof glass.
3. Where there is an alarm system, glass breaker sensors that detect glass breakage should be installed close to glass doors or windows. You should discuss annual testing of glass break sensors with your alarm provider.
4. Doorframes should be sturdy and appropriate for the door type. Weak frames should be replaced or rebuilt.
5. Exterior door locks should conform to guidelines found in the section on locks.
6. Interior or office doors should be equipped with heavy-duty, mortised latch sets with dead-bolt capability. Rim-mounted, deadbolt, or drop-bolt locks can be installed to increase security of important offices or rooms.
7. Doors with external or exposed hinges may be vulnerable to pin removal. The hinge pin should be made non-removable by spot welding or other means, or the hinges should be pinned to prevent separation. Such exits should be alarmed and used only for emergencies.
8. Staff should not be allowed to exit through back doors which lead to alleys or unusual streets.
9. 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 explosive devices.

10. All exterior doors without glass vision panels should be equipped with wide-angle viewers, or peepholes, mounted at a height accessible to tall and short individuals.
11. Interior doors should have two-way visibility at stairways and corridors. There should be a clear view of room interiors from the doorway.
12. Access to offices, kitchens, electrical, mechanical rooms, and storage rooms must be limited to appropriate staff and locked when not in use.

- ***Windows***

Windows should provide light, ventilation, and visibility, but not easy access for intruders.

1. Glass block can be used to seal a window, allowing a continued light source while providing increased security, although visibility and ventilation will be diminished. Local building codes should be consulted regarding placing glass block in rated corridors, egress paths, or building occupancies to ensure conformance to applicable fire ratings.
2. Gates and expanded steel screens, while often unattractive, 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.
3. Skylights, roof access, 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.
4. *A critical note on glass*: Flying glass can be as dangerous in an explosion as the actual explosion. Consider replacing traditional glass with safety or shatter-resistant glass, or using a clear protective film to secure the glass to the frame.

- ***Fencing***

Fences make an intruder's entry more difficult and give the appearance of a secure institution. When considering any protective element, institutional building owners, administrators, and facility managers should consult local building and zoning codes regarding installation of fences, prior to planning, design, and construction.

In keeping with the planning principles of crime prevention through environmental design (CPTED), uses of fencing, natural site features, and perimeter site lighting are relatively low cost, low-tech opportunities to reduce problems and enhance security.

1. All physical barriers added to an institution should be compatible with the aesthetics of the neighborhood or surrounding environment. Institutions should make every effort to avoid alienating neighbors who may serve as part of a neighborhood watch and provide additional "eyes and ears" to the overall security program.
2. Open ornamental fences, unlike walls, do not block visibility, are less susceptible to graffiti, and are more difficult to climb.
3. Fences should be at least six feet high. Institutions should take advantage of any small incline or hillock along which to build the fencing.

4. Fences should be designed to prevent a person from reaching in with their hand or a wire to open the fence gate from the outside.
5. 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.
6. Walls should be constructed where there is a need for privacy and noise control.
7. 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.
8. Keep shrubs low, less than 36 inches, or clear them away completely. Cut back vines attached to buildings to prevent determined intruders from gaining access to upper windows or unprotected roof access.
9. Creating an impenetrable physical barrier unprotected by personnel is difficult. Even when protected by personnel, people grow fatigued, inattentive, bored, and make mistakes.

- ***Protective Lighting***

Adequate lighting is a cost-effective line of defense in preventing crime. As with all other aspects of design and construction, institutional building owners and facility managers should consult with a security professional, licensed architect, engineer, or lighting consultant to determine locations and the best type of lighting for each institutional site.

1. Interior and exterior lighting can be provided without being intrusive to neighbors.
2. All entrances and fences should be well lit.
3. For outside lighting, the rule of thumb is to create light equal to full daylight
4. Light should be directed downward, away from the building or area to be protected and away from security personnel patrolling the facility.
5. Where fencing is used, lighting should be inside and above the fencing to illuminate as much of the fence as possible.
6. Lighting must be consistent to reduce contrast between shadows and illuminated areas. Lighting levels should be uniform on walkways, entrances, exits, and in parking areas.
7. Perimeter lights should be installed so the cones of illumination overlap, eliminating areas of total darkness if any lamp fails to light.
8. Lighting fixtures should be vandal-resistant. Repair and replace defective or worn-out bulbs immediately.
9. Prevent trees or bushes from blocking lighting fixtures.
10. Timers and automatic photoelectric cells protect against human error, and ensure operation during inclement weather, even when the building is unoccupied.

EXPLOSIVE THREAT PLANNING

For additional information please refer to these websites:

1. www.threatplan.org
2. www.adl.org/security

- ***Physical Security***

  The best way to secure an institution from explosives is to prepare a physical security plan. Institutions must take all responsible steps to prevent the introduction of an explosive into the environment. The first step in creating an explosive threat response plan (ETRP) is preparing a physical security plan to prevent the planting of any device. Since no physical security plan is foolproof, even the most secure institution should have an ETRP. Aspects of physical security relating to explosives:

  1. Offices and desks should be kept locked, especially those unused and unoccupied. Utility and janitorial closets should remain locked at all times, as should access to boiler rooms, mailrooms, computer areas, switchboards, and elevator control rooms.
  2. Identify and secure potential hiding spaces for explosives. A device does not have to be large to cause severe physical and psychological damage.
  3. Trash receptacles, especially dumpsters, should be kept locked, inaccessible to outsiders, and far away from buildings. The areas around these items should remain free of debris.
  4. Cars and trucks should be required to maintain a safe, 50- to 100-foot 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 the building. When planning new facilities, create as deep a setback, known as standoff distance, as possible.
  5. Consider using blast-resistant walls and shatterproof, blast-resistant windows to block the effects of a blast.
  6. Shrubs and other plants and trees should be trimmed, so they will not provide a hiding space for explosives and those carrying them.
  7. Employees should be encouraged to maintain tidy work areas so that they or their coworkers will notice if something is out of place.
  8. Flying glass is a grave source of danger in the event of a blast. Consider minimizing glass panes, and coating with shatter-resistant film.
  9. More than one exit may be damaged in a sufficiently large blast. Plan for several alternative emergency escape routes. Practice evacuation drills with building occupants.
  10. Examine the local area to identify risks from neighboring institutions and potential targets.

Mail and Delivery Protocols

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.

1. Conduct a vulnerability assessment to determine if your organization or a particular employee is a potential target.
2. Appoint a mail center security coordinator and an alternate to be responsible for the developed plan and to ensure compliance with it.

3. Establish direct lines of notification and communication among the mail center security coordinator, management and your general security office.
4. 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.
    a. What should you look for in a suspicious package?
        i. Excessive postage
        ii. Misspelled words
        iii. Addressed to title only (e.g., President)
        iv. Rigid or bulky
        v. Badly-typed or written
        vi. Strange odor
        vii. Lopsided
        viii. Oily stains on wrapper
        ix. Wrong title with name
        x. Protruding wires
5. Develop specific mail center handling techniques and procedures for items identified as suspicious and dangerous.
    a. If a package looks suspicious, what should you do with it?
6. Develop verification procedures for confirming the contents of suspicious packages encountered through the screening process. If you receive a suspicious package, it may useful to call the addressee to see if they are expecting something.
7. Establish procedures for isolating the suspicious package. At the least, identify an isolated room or area to place suspicious items to hold them 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 device in cabinets or drawers).
8. Conduct training sessions for mail center, security and management personnel to ensure that all phases of a mail bomb screening program work.
9. Conduct training for all employees of the institution to look for suspicious mail and packages.
10. Conduct unannounced tests for mail center personnel.

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

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

Unwarranted Interest in your Organization

Many terrorist organizations first engage in surveillance on their potential targets. Thus, you should pay attention to anyone attempting to photograph, film or study your facilities—especially in the days and weeks leading up to special events.

Someone examining your facility (or looking closely at the people arriving 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 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. Every institution should be encouraged to have a camera available to take photos of suspects. Inexpensive disposable cameras will suffice but do require that the photographer get closer to the subject.
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. The response may be, "None of your business, I can take pictures of whatever I want." This is true (unless the person is trespassing) but 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. 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.

Receipt of Phoned-In Threats

The bomb threat is an all-too common form of harassment against communal institutions. Responding to such threats requires careful planning and rigorous practice.

6. 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 take.
7. **Telephone switchboard personnel** (or all personnel who receive direct calls from outside the institution) should:

a. 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.
b. Do not irritate or insult the caller.
c. Do not slam down the receiver
d. Try to have a second person listen in on the call. A covert signaling system should be implemented or a recording device installed.
e. 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.
f. Keep the caller on the line for as long as possible. Consider asking the caller to repeat information.
g. Record 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.
h. **Remember**: during a bomb threat, use no devices that generate radio signals, such as cell phones, walkie-talkies, etc

8. Information to be sought by the threat recipient includes:
   a. **IN AN EMERGENCY use the Explosive Threat Call Checklist provided in this booklet**.
   b. If the caller does not provide it, ask the caller WHEN the explosive will go off and WHERE the explosive is located.
   c. Ask the caller to repeat as much information as possible, this way you can keep him/her on the phone
   d. 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.
   e. 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.
   f. Listen closely to the caller's voice. Record that information on the Explosive Threat Call Checklist.
   g. REPORT the information immediately.
   h. Remain available for questioning by law enforcement.

Evaluation and Decision

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

1. 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.
2. 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.
3. Get your command and communications centers (primary and secondary) up and running.
4. Determine likely targets. Produce a master target list and use it in light of the information received in the threat in order to narrow a search.
5. Determine procedures to establish search patterns and track the progress of search teams.
6. Have building plans readily available.
7. 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

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 the use of copycat threats as a means to interrupt business and other 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.

Evacuate Immediately

Evacuation requires that you do three things:

1. Notify people of the intended evacuation.
2. Conduct the evacuation in a safe, orderly fashion.
3. Be flexible enough when creating your plan to allow the evacuation to proceed if normal egress routes are blocked, dangerous or damaged.

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 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, either alone or 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:

- If it is safe to do so, everyone should check over his/her own workspace to ensure nothing has been hidden in the work area.
- 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 more safe and 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 two 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 into 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 Holidays and Other Special Events" on page 113.)
  - 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 and 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.

Law enforcement Response

An ETRP requires an understanding of precisely how local law enforcement 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 the 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 planning, and underscores the need to build relationships with local law enforcement well before a problem arises.

- ***Car and Truck Bombs.***

  Without extensive physical alterations and an extensive security program, defending against truck and car bombs is very difficult. Nevertheless, well-planned physical security precautions implemented by an institution represent an improvement over doing nothing at all.

Car and truck bomb prevention is a matter of physical security first, and search and evacuation second. The key defenses are excluding potentially dangerous vehicles from the institution, and, if they are admitted to the grounds, keeping them far enough away to prevent damage.

The institution may consider adding physical barriers, such as concrete Jersey barriers, between the street and the facility. In an urban environment where on-street parking is close to the facility, consider requesting no-parking designations from the local police department. Some other tips:

1. Restrict parking closest to building, by eliminating parking or limiting parking to staff and key lay-leader vehicles. Institutions may choose to issue a windshield identification sticker to determine who belongs and who needs further scrutiny.
2. Train staff and security personnel to be aware of types and appearance of vehicles used in these incidents.
3. Use barriers, gates, and fences to prevent access to the facility by unauthorized persons.
4. Cars and trucks should be required to maintain at least a 50- to 100-foot 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 the building.
5. Consider using blast resistant walls and shatterproof, blast-resistant windows to block the effects of a blast.

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

Identifying Car and Truck Bombs. Car and truck bombs might be identified by the outward appearance of the vehicle, behavior of the driver, and other suspicious indicators, including:

1. The vehicle's driver does not enter the facility, but rather runs or walks away.
2. The car or truck appears to be sitting very low on its springs, indicating great weight.
3. The car or truck is parked illegally or too close to the building. The facility should restrict parking closest to the building.
4. Older cars and trucks, and rental vehicles, are more likely to be used in a car bombing. Be wary of any type of vehicle appearing to have been abandoned, such as an expired or missing inspection sticker, registration, or license plate.

None of these items are indicators of potential violence, and many are consistent with innocent behavior. However, they are clues to observe and consider for truck bomb security

- ***General Target Hardening***

Visible security devices and technology, such as lighting, fences, CCTV, and alarms, make a facility look less inviting to a potential attacker. Target hardening is based on the premise that the more one's facility looks difficult to enter, the more likely a perpetrator will move on to another target or lose their nerve to attack yours. Some hardening tips:

1. Signs indicating the presence of an alarm system
2. Visible security patrols and vehicles
3. Well-maintained perimeter fencing and lighting
4. The general appearance of a well-maintained facility
5. Regular presence of local law enforcement on or near the grounds

EVENT SECURITY

Security for events, such as meetings, fundraisers and other public activities, require extensive planning. 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 event venue. 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.

Steps for securing an event include

1. Assessing Risk. A number of elements go into any risk assessment; however, three stand out:
    - the existence of prior threats or incidents,
    - the extent to which the event is open to the public, and
    - the extent to which the event is publicized.

1. Establishing a 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).Once you have identified your perimeter, you should identify every way in and out of that perimeter. Including entrances, emergency exits, kitchen doors, windows, and your security screening area. Once your perimeter is established, 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.

2. Create a security screening center. You will want to be able to secure the area so that anyone who wants to enter must go through your security screening checkpoint. 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. Considerations include:

- Every possible way into the security perimeter must be *locked, guarded, or alarmed.* Remember, you must do this consistent with the fire code.
- Someone should be in charge of maintaining the perimeter and 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 (e.g., by a medical emergency). Guards must understand that they are guarding an event, not participating in it or watching it. Therefore, they should be watching the crowd and the perimeter and should not focus on the performer, speech or event.

In event security, as in all things it is critical to remember that you are bound by local, state and federal law pertaining to discrimination and public accommodations and the fire codes.

POST-INCIDENT

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. We urge you to plan for this ahead of time.

- ***Command control and communications***

  As we have explained elsewhere, 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. Some thoughts:

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

6. The media may be interested in your incident. They may also be the most effective way to communicate important information to constituents. Depending on where you are, media may be more or less receptive to becoming a conduit for relaying information.
7. 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.
8. 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.")
9. 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-xxxxxxx," "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.
10. 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 copycat or not, and/or to ensure that an ongoing investigation is not otherwise damaged.
11. 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.

- ***Disaster recovery***

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

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

- ***Evidence***

  There is a powerful temptation after discovering damage or graffiti to clean it up immediately. We urge you to resist that temptation and leave the entire crime scene untouched until the police arrive. By waiting, you help ensure that valuable evidence is not lost – and that the perpetrators are caught.

CONCLUSION

Community facilities can remain open and welcoming to their members, and occasionally, to the public, while remaining alert and prepared for any type of emergency or threat. Building relationships with local law enforcement agencies will enhance crime prevention efforts and establish critical networks well before a disaster or in the event of an emergency.

For additional information – and for more detail on any of the topics covered here – please visit www.adl.org/security or contact your local ADL regional office.