ADL GUIDE TO PROTECTING YOUR RELIGIOUS OR COMMUNAL INSTITUTION

ADL
Anti-Defamation League®

Anti-Defamation League

Marvin D. Nathan
National Chair

Jonathan A. Greenblatt
CEO

Kenneth Jacobson
Deputy National Director

Steven C. Sheinberg
Chief of Staff
General Counsel
Senior Vice President, Privacy and Security

Glen S. Lewy
President, Anti-Defamation League Foundation

Deborah M. Lauter
Senior Vice President, Policy and Programs

Steven M. Freeman
Deputy Director, Policy and Programs

Bonnie S. Michelman
Chair, Communal Security

THE LAW ENFORCEMENT, EXTREMISM AND COMMUNITY SECURITY UNIT

David C. Friedman
Vice President, Law Enforcement, Extremism and Community Security

Kara K. Chisholm
Director, Institutional Advancement for Law Enforcement, Extremism and Community Security

Oren Segal
Director, Center on Extremism

Elise M. Jarvis
Associate Director, Law Enforcement Outreach and Communal Security

For additional and updated resources please see: **www.adl.org**

TABLE OF CONTENTS

NOTICE: This guide is intended to help institutions become aware of basic security considerations. It is not 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 the use, non-use or misuse of this information.

Note: The guide has been developed for groups of all sizes and types. As such, it uses words like "institution," "organization" and "group" interchangeably. The same is true for words like "facility," "property" and "premise."

INTRODUCTION

The unfortunate reality is that any religious or communal institution may become a potential target for extremists, shattering their sense of comfort and safety. Organizations have the responsibility to do everything possible to protect themselves and their constituents from potential threats. The Anti-Defamation League (ADL), a civil rights organization founded in 1913 to fight anti-Semitism and all forms of hate, has been providing security guidance to Jewish institutions for decades. This manual was created to share security best practices with other religious and communal institutions.

In addition to the information provided in this manual, ADL can be a resource to your institution, through our expertise and experience as the most important non-governmental authority in the United States on hate crimes, hate groups, extremism, cyber-hate, and terrorism. ADL works more closely with law enforcement than any other private organization in the U.S., training from 10,000-15,000 federal, state and local law enforcement personnel each year in these topics and areas, among others. ADL's Center on Extremism tracks and monitors extremists, ranging from white supremacists to homegrown Islamic extremists, providing law enforcement with critical information on a daily basis. Headquartered in New York City, with 27 regional offices across the country, ADL is positioned on the ground to help your institution respond quickly and connect with the appropriate authorities, should your organization be targeted or threatened.

Whether your organization has not had to face a security threat in any significant way before, or you need to update and expand the security measures you already have in place, this guide can be of help. It was specifically created by ADL experts to help you think through the basic considerations all institutions need to take into account.

This guide was written with many different types of organizations and institutions in mind. You may not find that every point is relevant to you, but you may find that many of the items are still useful when developing your own security plan. Additionally, we urge you to share this guide with selected members of your staff and the leadership of your organization, as well as with a security professional who can assess your institution firsthand.

Chapter 1

SECURITY PLANNING

If you don't already have an overall security plan in place, it's likely that your organization has handled any incidents as they happened. Hopefully, you were lucky, and the right people were in the right spot to make the appropriate decision so that you had a positive outcome. However, think about how much safer and easier it would have been if you had a plan in place.

A sound security plan means that an institution will be in a better position to thwart and, if necessary, recover from a security breach, be it a physical incident or a digital one.

Security planning is a long-term process which involves consultation with, and the training of, many members of your community. While no guide can provide a security plan for each institution, there are some considerations all institutions must take into account. 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]

Basic Considerations

- Not all institutions encounter the same risk, but all encounter some risk.
- Making security a top priority needs to be a part of the culture of all our institutions.

[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.

- When developing a security plan, your leaders and the professionals who work for your organization should assess the risks to your organization and its members, as well as the physical property, the surrounding neighborhood and the way information is handled. You should seek professional guidance if necessary.
- Leaders must make sure that security is part of your institution's culture. At the very least, you should seek input on security from all of your staff as their buy-in is essential for a smoothly running plan. They are also your critical "eyes and ears."
- Staff, leaders and community members must be motivated and educated to understand the need to create and implement a security plan.
- 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 must help them understand the importance of the security plan and their role in that plan. Community members should:
  - Be watchful, ready and willing to report suspicious activity.
  - Be aware of their surroundings.
  - Report anything out of place, missing or that does not appear to belong.
  - Actively cooperate with security directions, procedures and policies.
  - Share ideas and suggestions about security and safety.
  - Actively work to create a culture that is both secure and welcoming.
  - Support the leaders of the organization and the staff as they make the difficult decision to create and implement an effective security plan.

It is important to note that creating a plan is just the start of the process. Once the plan is written, it is important to make sure that all leaders, employees and members of your community know what the plan is and practice the steps before an event occurs. Everyone should also review the plan on a regular basis and remember to implement it continually, without exception. Regular training and updating your security plan are also 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 or hire a professional security firm for assistance in this process.

Assessment

Taking stock of the current situation and understanding what potential threats there may be to your organization is of paramount importance. First, determine current risks, then identify who or what needs protection from those risks and, third, begin working with professionals so you know what measures should be taken.

- **Identify Threats**. First, you must assess the danger to your institution. Here are some helpful questions to answer so that you can identify 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 the local ADL Regional Office say about extremist activity in your area? (ADL monitors and has information about all types of prejudice, bias and hate crimes, not just those related to the Jewish community.)
- **Identify Targets for Protection**. Identify who and what you need to protect (e.g., people, property and data) and understand what makes those things vulnerable. Keep in mind that you will need different strategies for protecting children, adults, property and data; your planning must account for all of them.

  Note also that sometimes these targets are related and what affects one can also affect another. For example, a network breach that compromises membership lists and payment information can create problems for your members, but it also can do great damage to your institution's reputation.
- **Relationships with Law Enforcement.** We urge you to recognize the importance of developing and maintaining a working relationship with your local law enforcement agencies, as well as other emergency services in your area. As you'll see in the next

chapter, your local professionals can provide helpful and insightful information on how to create and implement your security plan. (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.)

Planning

- **Risk Reduction.** Once you have identified the most appropriate measures to reduce your risk (recognizing that you can never eliminate all risk), begin implementing the steps as soon as you can. For example, the first step to better control access to your office or building might be to replace or re-key your locks.
- **Command, Control, and Communication** are your three keys.
  - — Identify a decision-maker with the authority to act. Make sure that others know and respect that he or she is in charge.
  - — Ensure that decisions can be effectively communicated to those who need to know.
  - — Plan for contingencies in case a designated decision-maker is unavailable during an emergency, whether they are out sick, on vacation, at lunch, or away from the office for a meeting. Develop a succession list or chain of command in the event of an absence, even a temporary one.
  - — Be able for all present, as well as your organization's leadership, to ascertain who is in charge at any given point, whether it is the designated decision-maker or someone else in the chain of command.
  - — Create a simple, user-friendly form to document incoming threats. Include a checklist identifying the type of threat, the person making that threat and the method used to deliver the threat: phone, mail, site visit or other means. Leave space for additional comments, such as identifying characteristics.
  - — This checklist will help your staff when they are speaking with law enforcement, should an investigation be needed. (Women's health clinics and at-risk facilities use this approach to document ongoing threats.)
- **Varied Use Plans.** Create plans to address 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.

Immediate Security Steps

There are several basic measures that should be implemented right away, even before your full security plan is developed:

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

- **Have all emergency phone numbers readily available.** While you should always try to contact 911 first in any emergency, you should also have the phone number of your local emergency responders readily available. In addition, 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 a landline instead.)*
- **Utilize the security devices you already have. Ensu**re 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.
- **Use available resources to document suspicious behavior.** Smartphones, electronic tablets or other devices can be extremely helpful for taking pictures or videos (when it is safe to do so) that may assist police if a suspicious individual or car is seen.

Implementation of Your Security Plan

Implementing a security plan requires **Accountability, Updating, Training and Relationship Building**.

- **Accountability**
  - — Designate a staff member as security manager, accountable for implementing, reviewing, and constantly updating the security plan.
  - — 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, including maintenance personnel.
  - — 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.
- **Regularly Update Plans and Procedures.** A security plan must constantly be reassessed and updated. A stale plan is no better than — and can be worse than — no plan at all.
- **Training.** 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.
  - — Discussion-based exercises, including orientation sessions, workshops and tabletop drills familiarize staff and community members with your various security procedures. In tabletop drills, response teams are presented with a crisis scenario. Specific roles and responsibilities are reviewed and in-depth, constructive, problem-solving discussion "walks" the team through the scenario so that potential issues can be identified and resolved.
  - — Emergency drills practice specific procedures or protocols. The intent is to ensure that all potential participants know what they are to do in an emergency.
  - — Functional exercises simulate emergency situations. They are time-sensitive, interactive events in which participants receive directions from an exercise controller and respond appropriately (as if there was an actual emergency event). The exercise is then debriefed, and recommendations are made for improvements to security and response procedures.

- **Build Relationships**. At every stage of security planning, build relationships with the local emergency services. (More on this in the next chapter.)

Chapter 2

BUILDING RELATIONSHIPS WITH EMERGENCY RESPONDERS

Your organization may already have a contact at the Police or Fire Department, but many groups have not yet built a rapport with their local authorities. Asking the authorities and emergency personnel for help in the planning and implementation of a security plan is important. And, police and fire officials know that involving them in your process is also of great benefit to them if there is an emergency to which they have to respond.

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

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

Get Acquainted

Communication is the key to a successful relationship with the authorities and working with them will enhance their ability to serve your needs. It's important to recognize the extraordinary service all of these individuals provide our communities and be mindful of their time and other commitments. 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.

- **Invite police, fire and other emergency personnel to visit your building or office** so

they may become familiarized with the premises, personnel and standard operations. Not only could this provide useful information to all parties, but it will also help begin building a relationship with the first responders who would deal with an incident at your facility. The worst time to meet your local officers for the first time is during a crisis.

- **Share blueprints and floor plans of your facility** with all your local emergency responders. If they are unwilling or unable to keep them on file, consider having the plans stored in a secure nearby, off-site location for quick access during an emergency.
- **Check with emergency responders to determine what other information they will need** and where they believe that data should be safely stored.
- **Create a "go-to" plan** that can provide emergency responders with the information they may need. Include another copy of your floor plan and information on where important assets are located.
- **If your facility has a gym or a similar "entertainment" area,** you may wish to invite local police officers and members of the firehouse to use it.
- **You can also invite local emergency responders to join your members for various activities:** a weekly religious service, holiday festivals, celebrations, special events and community meetings.

Law Enforcement

- **Invite an appropriate representative of the police department to your initial security planning meeting**. Share your specific concerns and ask for actionable suggestions on how to communicate during an emergency, create evacuation plans, etc.
- **During special events (including religious holidays), keep your local police department informed** as to the times and the nature of your event. It is also useful to advise them about when people are typically walking or driving to and from your institution.
- **If your local department has a special weapons and tactics team (SWAT),** consider

having a SWAT officer map your institution and its property to determine what information would be helpful in the unlikely event that a SWAT team is deployed.

- **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 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; make sure that you are kept apprised of changes in law enforcement staff and responsibilities. When there is a change, start building the new relationship as soon as you can and remember to keep your current relationships fresh and vital.

Fire Department

- **Meet with local fire officials** and a member of the arson squad.
- **Ask that someone review your facility and its fire plans**. Once any suggested revisions or additions are made to your plans, remember to update your "go-to" plan accordingly and share it with all appropriate emergency responders.
- **Meet with your local Emergency Medical Technician (EMT)** representative to help create a medical emergency plan. In addition, you may want to consider first aid and CPR training for your staff. At the very least, you will want to have an emergency medical kit (or kits) on hand, as well as an automated external defibrillator (AED).

Chapter 3

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. There are three often interrelated ways in which this basic premise is implemented:

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 dissuaded from trying to enter your premises because they decide it's too difficult to enter and leave voluntarily.

There are a number of elements to physical security. Among them are:

Access Control

Access control is essential to your institution's security plan as it means when the facility or office is open, no visitor, delivery, service person or unknown individual can enter the facility without being directly or indirectly observed and approved. Your security plan should develop and implement policies to ensure that screening is ongoing so that no one enters your building unscreened.

It's important to make these systems a part of your institution's culture. A culture that promotes security consciousness allows staff and visitors to understand that minor inconveniences may translate into major security benefits.

There are many ways to screen using human resources, like ushers, volunteers, paid staff,

hired security guards, etc., and electronic devices. The installation of closed-circuit TV cameras, intercoms and door release systems can significantly assist in the screening process.

Some key tactics for access control are:

- **Minimize the number of open entrances** to your facility (consistent with fire codes).
- **Monitor entrances**. It is easier to prevent entrance into your building than it is to get someone to leave. Ideally, an institution or office should have a single entrance that is monitored by a staff person and equipped with an intercom system for communicating with anyone who comes to the door. External barriers and locking the door at all times may also be considered.
- **Have a staffed security desk.** Establish a protected security desk in the main lobby of each building or office with an open access or open door policy. Use a sign-in/out logbook and have the supervising employee check credentials (see below).
- **Check credentials.** Before allowing individuals to enter your property or offices, check that their identification papers or other credentials, including membership cards, are valid. It is perfectly legitimate to ask for photo identification. Some words of caution:
  - Employees cannot always tell the difference between valid and forged documentation. Police and most utility employees carry credentials, but staff may not be able to distinguish accurately between real and fake IDs.
  - A uniform or serviceperson's identifying 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 appropriate 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.
- **Use photo IDs.** All institution or organization employees should have identification cards to identify non-employees immediately and settle identity questions. If appropriate, you may choose to issue photo IDs to your membership as well.

- All employees should be required to wear their photo ID prominently while in the building and, for their own safety, kept from view when away from the building. This is to prevent theft. Additionally, there is no reason why any person on the street or public transportation should be able to identify who someone is and where he or she works.
- Photo identification should not be issued without accompanying education about its care, including the procedures to follow if a card is 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.
- Lost cards should be reported immediately.

- **Monitor visitors after entry**. At no time should visitors be allowed to roam freely. They should be escorted or observed. Special diligence should be applied to individuals who work on the organization's most sensitive systems such as burglar alarms, fire alarms, communication systems or computers. In larger institutions, certain areas should be considered off-limits to all but authorized personnel.
- **Clearly identify open access boundaries.** Community centers for youth and seniors, facilities with gymnasiums, and other similar institutions desire to maintain open and free access to those areas. But, allowing visitors free access to that portion of your facility doesn't mean they should be allowed to go anywhere. The end of open access areas should be marked as such. So should restricted areas or office spaces. Visitors should perceive that institution personnel are observing their presence and actions.
- **Prevent stay-behinds.** End-of-day locking procedures should include a visual examination of all areas of the institution to prevent "stay-behind" burglars or others preparing to do harm in some way.

Key Control

The term key control relates to all types of access to buildings and individual offices or

spaces (specific locks, key card access and knowledge of alarm codes). A key control policy is essential to a sound security program. Failure to consistently track those who have the ability to enter locked areas on their own can become a problem and defeats the purpose of a security system. Remember that disgruntled former employees or volunteers may break into a building to burglarize or otherwise harm your facility.

- **Have a registry.** A central key control registry should be established for all keys and combinations. Employees and organizational leaders should be required to sign them out. Key return should be part of ending service and exit interviews, if applicable.
- **Have an approval process.** Supervisory approval should be required for the issuing of all keys and locks. Spare keys and locks should be kept in a centrally located locked cabinet, supervised by a designated employee. Master keys should be issued to a restricted number of employees and should be checked at least twice each.
- **Consider rekeying.** When access to keys, cards, etc. is not well controlled, or keys and cards are lost, changing the institution's locks or access readers (also called rekeying) may be worthwhile.
- **Change lock combinations and codes regularly.** 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. The combination should also be kept under strict management control.
- **Use locks with keys that can't easily be duplicated.** It is good policy to use locks that require special key blanks for creating additional keys.
- **Consider installing key card readers.** Although they are expensive, key card readers make for more effective access control and are nearly automatic. Large institutions, or those with valuable assets, may find key cards worth the investment because they can control and track who enters and exits specific rooms at any time.

Locks

Durable locks are essential to building and operational security. We recommend consulting with an experienced locksmith who can assess your institution's circumstances and

provide specific recommendations. The following information should aid in starting your discussion with a professional:

- **Deadbolt locks** are the most reliable. They should sit at least an inch into the door frame or lock-bolt receiver and be installed with the proper strike for the type of door frame (wood versus metal).
- **Padlocks** should be of high-grade material designed to withstand abuse and tampering.
- **Lock cylinders** should be highly pick-resistant.
- **The door-locking system** must meet applicable life safety and fire codes to allow emergency exiting without impediment. It's important to keep abreast of any changes in your local laws.
- **The door jamb** must be sufficiently strong as a strong lock entering a weak jamb will fail.
- **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.
- **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.
- **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 is critical.** The institution's security manager or a designated staff member with training should:
  - Regularly inspect and report all damaged locks and ensure that they are repaired quickly.
  - Establish a chain of responsibility for all locks on doors and windows to ensure that they are indeed locked. This responsibility should include the reporting of all failures to do so.
  - Ensure that keys are not left unattended.

— Recommend installation of additional locks where necessary.

— Add the locking key control program as part of the periodic security audit. Remember to survey all lock locations. In addition to exterior locations into the facility, locks should be present on interior doors, windows, offices, filing cabinets, and storage closets.

Protective Devices, Alarms, and Technology

Protective devices are an important consideration in strengthening security. They include intrusion, fire detection and alarm systems, as well as cameras connected to a closed-circuit TV (CCTV) system. These can be costly, and there is a wide variety of models, manufacturers and features to choose from, so selection, specification, and installation require professional advice.

You will want to begin by contacting local law enforcement and requesting help from the unit that specializes in crime/burglary prevention as its officers are specially trained and can offer expert guidance. Additionally, 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.

Here are some guidelines that may prove helpful in fostering discussion with the experts you consult or in upgrading your existing equipment:

Alarm Systems

Like locks, alarm systems require professional guidance. The size, location and type of institution will determine the type of system required, but here are some initial guidelines for installing and maintaining alarms:

- Ensure that the alarm system meets local legal and code requirements.

- Determine if the city or town allows direct-dialing the police when an alarm is tripped.
- Ensure that all alarm systems have emergency backup power sources.
- Conceal the alarm control box and limit access to it.
- 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.
- Protect all wiring components and sirens from tampering.
- Test the alarm system regularly to maintain effectiveness.
- Post stickers about the presence of alarms in windows, and at entrances and exits.
- Teach your staff and organization's leaders how to use the equipment and work with the monitoring company.
- Consider adding panic buttons to the system, so that alarms can be triggered from locations other than the main alarm panel. Place them in key offices, spaces used during off hours and in locations where intruders may first be confronted, such as reception areas.
- Consider the use of personal or handheld alarms as well. They emit a loud, warning sound that alerts others and guides them to the source of the alarm (i.e., the location where help is needed).
- Motion detectors or automatic sensors that respond to sound are excellent protective devices, used alone or in conjunction with your lighting system. These detectors and sensors are economical and can be used inside or outside the building.
- Alarms using magnetic contacts and trip wires are also effective, and they are economical, but alarms with motion, sound, or light detectors are usually more dependable. The cost invested in a dependable alarm system is generally less than the cost of damages caused by an intruder.

CCTV Systems

Surveillance cameras can document criminal acts occurring on your property, which can later be used to identify and prosecute perpetrators. They can also serve as a deterrent to potential intruders. Although initial costs are often expensive, in the long run, cameras and the recording equipment are economical when compared to the costs of potential losses or harm to staff and group members.

- To be effective, CCTV systems must be properly maintained and monitored. The people responsible for monitoring or reviewing the video must be well trained and focused. Distractions should be minimized at least, eliminated if possible.
- Most institutions are unlikely to have the resources for continual monitoring, but the majority of systems now have video storage capability that allows institutions to check and review footage after the fact.
- Use wide-angle lenses to survey entrances.
- Use cameras with infrared illumination to enhance nighttime video.
- Couple the cameras with a time-lapse recorder for permanent records.
- Make sure cameras have a time and date recorder.
- Compare the cost of color versus black and white and determine the cost/benefit ratio based on your organization's security needs.
- Save footage for a minimum of 72 hours if any suspicious behavior is noted. Often, it is worthwhile to hold onto the footage indefinitely in case the police or the courts need it for evidence.
- Consider upgrading older cameras to newer hi-definition models.

When renovating, upgrading, or modifying existing facilities (and especially when designing new facilities), a licensed architect and engineer should be consulted with your security issues in mind. You will want the professionals to recommend specific appropriate, code-compliant (applicable local life safety, building, and fire codes) for windows, doors, screens, gates, skylights and building construction materials. Best

practices for physical upgrades of this type are:

Doors

- All exterior doors, main building doors and lobby doors leading to common corridors should meet several important criteria.
  - Solid core, wood, or metal are acceptable, depending on code requirements.
  - Glass door panels or side panels should be reinforced with metal or steel mesh or replaced with shatterproof glass.
- Sensors that detect the breaking of glass should be installed close to doors made of that material and windows. You will want to discuss annual testing of such glass-breaking sensors with your alarm provider.
- Door frames should be sturdy and appropriate for the door type. Weak frames should be replaced or rebuilt.
- Exterior door locks should conform to guidelines found in the section on locks.
- Interior or office doors should be equipped with heavy-duty, mortised latch sets with deadbolt capability. Rim-mounted, deadbolt or dropbolt locks can be installed to increase the security of important offices or rooms.
- 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.
- Staff should not be allowed to exit through back doors which lead to alleys or unusual streets.
- Doors to utility closets should be equipped with deadbolts and kept locked at all times. If unsecured, such closets can become hiding places for “stay-behind” criminals or explosive devices.
- All exterior doors without glass vision panels should be equipped with wide-angle viewers or peepholes, mounted at a height accessible to both tall and short

individuals.

- Interior doors should have two-way visibility at stairways and corridors. There should be a clear view of room interiors from the doorway.
- Access to offices and kitchens, as well as electrical, mechanical 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.

- Glass blocks allow for a continued light source while providing increased security (although visibility and ventilation will be diminished).
- Gates and expanded steel screens are often unattractive but provide a high degree of security. Local building codes should be consulted regarding placing blocks or screens in fire-resistance rated corridors, egress paths or building occupancies restrictions to ensure conformance to applicable fire ratings.
- 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.
- A critical note on glass: In an explosion, flying glass can be as dangerous 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.

Environmental Design (CPTED) Elements

The planning principles of crime prevention through environmental design (CPTED) include the use of fencing, natural site features, and perimeter site lighting as they are relatively low-cost, low-tech opportunities to reduce problems and enhance security.

All physical barriers added to an institution should be compatible with the aesthetics of the neighborhood or surrounding environment. You 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.

Additionally, as with many of the other security measures mentioned in this book, you should consult with a security professional, licensed architect or engineer when installing CPTED elements.

Fences and Security Walls

A fence makes it more difficult for an intruder to gain entry and gives the appearance of a secure institution. As when considering any protective element, before planning, design, and construction, you should consult local building and zoning codes regarding the installation of fences. In general:

- Open ornamental fences, unlike walls, do not block visibility, are less susceptible to graffiti and are more difficult to climb.
- Fences should be at least six feet high. Take advantage of any small incline or hill when determining where to build the fencing.
- Fences should be designed to prevent a person from reaching in with their hand or wire, so they can't open the gate from the outside.
- If a panic bar is required for emergency exit, a solid metal or plastic shield should be used on the inside of the fence gate.
- Instead of fencing, walls should be constructed where there is a need for privacy and noise control.

Landscaping

Landscaping and refuse along fence lines, sides of buildings or near entrance points could hide criminal activity or actually aid an intruder.

- Keep shrubs low (less than 36 inches) or clear them away completely.

- Clear away trees and vines that might aid climbers.

Note: Creating an impenetrable physical barrier, even one protected by security personnel, is difficult; when people grow fatigued, inattentive or bored they can make mistakes.

Protective Lighting

Adequate lighting is a cost-effective line of defense in preventing crime. It's wise to include a lighting consultant in your planning discussions to determine locations and the best type of lighting for each site.

- All entrances and fences should be well lit.
- Lighting must be consistent and uniform to reduce contrast between shadows and illuminated areas, especially in walkways, entrances, exits, and in parking areas.
- Lights should be directed downward, away from the building or area to be protected and away from the security personnel patrolling the facility.
- The recommended light level is one that is equal to full daylight.
- At the same time, it is important to be considerate to those around your institution. Adequate interior and exterior lighting can be provided without being intrusive to neighbors.
- Lighting fixtures should be vandal-resistant. Repair and replace defective or worn-out bulbs immediately.
- Where fencing is used, lighting should be inside and above the fencing to illuminate as much of the fence as possible. Also, ensure that trees or bushes are not blocking lighting fixtures.
- Perimeter lights should be installed so the cones of illumination overlap, eliminating areas of total darkness if any lamp fails to light.
- Timers and automatic photoelectric cells protect against human error, and ensure operation during inclement weather, even when the building is unoccupied.

Chapter 4

DETECTING SURVEILLANCE

Many terrorist organizations or people intending harm to someone or some group will first engage in surveillance of their potential targets. It's important to keep alert and pay attention to anyone attempting to photograph, film or study your facilities — especially in the days and weeks leading up to special events.

Who to Watch For

Be wary of anyone:

- Recording data about your institution by sketching, taking notes, videotaping or taking pictures.
- Sitting in a vehicle for an extended period, including after regular business hours.
- Loitering near your facility or in the lobby of your building or office.
- Arriving at your facility and presenting themselves as "workmen" without prior notification (they may claim to be contractors or service technicians, etc.).
- Demanding to deliver packages or other items to a specific office or person.
- Attempting to bypass your security, even "accidentally" (walking past a check-in desk or receptionist).
- Appearing to be measuring distances or mapping out your floor plan.
- Being uncooperative or dismissive.
- Pretending not to understand what you are talking about when challenged about their presence on your premises.

When Someone Is Flagged as Suspicious

If you spot someone you believe may be conducting surveillance of your facility, pay attention to details. What seems unimportant to you might be important to law enforcement or your security company.

Call the Police Immediately

It is crucial that the dispatcher or/911 operator be given *all* available information.

- Provide your exact address and location of the incident that has you concerned (receptionist area, leadership offices, gym, etc.).
- Other important items to report include a description of the suspicious individual:
  - Gender
  - Approximate height and weight
  - Clothing worn
  - Type of car and license plate number, if one is observed
  - Any unusual characteristics that would make the person or persons easy to identify
- This is one of those instances where fostering pre-existing relationships with the police can be of great help. In addition to calling 911, try to speak with one of your organization's contacts.
- If a dispatcher/911 operator does not consider your situation an emergency, inform them if you feel threatened and require assistance immediately. If the responding law enforcement officer refuses to take a report, call ADL.

Gather Proof of Your Suspicions

Consistent with your safety and personal comfort level:

- Consider photographing the person doing surveillance. Staff members are encouraged to take photos or video of the subject using a camera or smartphone if doing so would not place them in an uncomfortable or dangerous position.

- If your institution has a surveillance system that can be monitored or reviewed, make sure the person responsible for that function knows what to look for and obtains footage of the incident.
- If the suspicious person starts to leave before police arrive, you may choose to approach the individual and inquire why they are taking photos of the location, recording measurements, or otherwise acting in a way you find suspicious.
- While the person may be dismissive of your question ("None of your business" or "I can take pictures of whatever I want," [2] for example) you will have placed the person "on notice" that his or her actions were observed.
- Even if the person leaves, police should be informed and provided with a report. Ensure that your leaders and staff are apprised of all relevant facts about the incident so they can identify the suspicious person or persons if they return.

[2] This is true, unless the person is trespassing.

Chapter 5

MAIL AND DELIVERY PROTOCOLS

Mail and package security is also essential regardless of the size of your organization or institution. It is critical that you have safeguards in place to prevent or successfully handle suspicious packages and mail. As is true with other security measures, your first step is to develop a "mailed hazard response plan."

The key is to channel all mail and packages through a screening process, regardless of how they are delivered. Your objective is to ensure that every letter and package receives formal scrutiny. This includes items received through the postal service, overnight carriers, couriers, and individuals not well-known to the receiver of a package.

Develop a System

1. **Conduct a vulnerability assessment** to determine if your organization or a particular employee is a potential target. Remember it is always better to err on the side of caution.
2. **Develop specific screening and inspection procedures** for all incoming mail or package deliveries. At a minimum, ensure that all mail and packages are examined by **someone trained to evaluate them.**
3. **Appoint a mail center security coordinator and a backup.** They should be responsible for implementing the plan and ensuring compliance from all employees.
4. **Establish direct lines of notification and communication** among the mail center security coordinator, management and your general security office if you have one.
5. **Conduct training sessions:**
    - For the mail center, security and management personnel to ensure that all phases of a mail bomb screening program work.

- For all employees and volunteers to look for suspicious mail and packages.

What to Look For

- Excessive postage or tape.
- Misspelled words or badly typed or written.
- Unusual addressing, such as the use of title with no name (e.g., President) or the use of incorrect titles.
- No return address or unusual return address.
- Rigid, bulky or lopsided packaging.
- Oily stains on the wrapper or a strange odor.
- Protruding wires.
- Unknown powder or suspicious substance.

What to Do With Something Suspicious

Develop specific mail center handling techniques and procedures for items identified as suspicious and dangerous.

1. **Have verification procedures in place** for confirming the contents of suspicious packages.
2. **Confirm that a package or envelope is expected** and what the anticipated contents are by contacting the addressee.
3. **Contact the person or company mentioned** in the return address.
4. **If the package can't be easily verified or you are still concerned**, be prepared to take safety precautions. If you suspect the mail or package might contain an explosive or radiological, biological, or chemical threat:

- Isolate the area immediately.
- Call 911.
- Wash your hands with soap and water.

(See Appendix for more information.)

Chapter 6

COMPUTER AND DATA SECURITY

Computer hacking, malicious software programs and other digital threats mean an unsecured computer and data system may leave your organization, its individual members, possible donors and staff open to personal harassment and financial difficulties. Plus, it can damage your organization's reputation. Since your institution can be crippled by a computer attack before you even know it has happened, computer and data security should be an integral component of your overall security program.

Due to the complexities of these issues, it's recommended that you consult a computer security professional for the most comprehensive security plan.

Key Concerns

Today, most computers and mobile phones have some form of Internet connection, whether high-speed, wireless, dial-up, etc. That makes your data and equipment more susceptible to breaches and theft than ever before. If you have a website, it too is subject to data breaches or defacements that can hurt your organization's reputation and cause public relations nightmares.

In addition to specific threats from people and organizations that may have a problem with your organization, you need to be concerned with automated programs that scan the web for possible hacking targets. These programs seek known flaws in software, like outdated website coding and security protection, as well as "backdoors" through which someone could gain unauthorized access to your system. When the automated program finds a vulnerable connection, it reports that information back to the hacker or "black hat" who launched the scanning program.

That person may choose to breach your network to obtain information that can be used

for illegal purposes; it happens every day. Once your system is compromised, the hacker may have access to all the data on your network or computer (credit card information, in particular), use your system as a base to attack other systems, store hacker tools and pirated software, or even delete all your data.

Your system is also vulnerable to infection by malicious computer programs. These programs are indiscriminate and often enter the system by inadvertent user action, including being fooled by "phishing" scams that come in via email. Lax security by website administrators or hosting companies, malicious employee activity, inadvertent loading of dangerous software, or divulging passwords can also cause problems.

Practical Prevention

There are simple and inexpensive methods to prevent computer crime and vandalism. The advice that follows 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.

Email

- Discourage the use of personal or non-related business email addresses for institution correspondence.
- Discuss and initiate a codified policy for the use of institution-based email addresses, including who is entitled to have one and who is in charge of managing their distribution.
- Set up separate accounts for your officers, employees and key members or volunteers on your own email system. These accounts should only be used for institution business, communicating within your community of members and interested parties and external communication for the organization.
- It's recommended that you avoid using a person's name, location or any other online identity (Facebook, LinkedIn, etc.) in their institution-based email address when a

title or job identifier is available (human resources@, officemanager@, director@).

- Close individual accounts as soon as they are no longer needed (an officer's term may end, volunteers may stop participating in your organization's activities, etc.).
- When sending an email to a large list of recipients, place the recipients' email addresses in the "bcc" (blind carbon copy) area of the addressee section. This will prevent member names from being revealed if the email is forwarded to a third-party.

Website

- Avoid having your website reside on an institution or member's home computer. Work with a professional web hosting company instead.
- Ask your web hosting service about security protocols, active backup of the website, procedures for Denial of Service (DoS) attacks, and unauthorized website access. Also, ask if they have a disaster recovery procedure that includes a 24/7 point of contact for emergencies.
- 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.

Social Media

- Appoint someone to serve as social media manager and have them control who has access to your social media accounts. Limit the ability to post to a few individuals, if not just your social media manager.
- Constantly monitor your accounts for threatening or otherwise inappropriate posts or messages. Remember that social media accounts can get hacked.
- Also monitor for hashtags (# and a word or phrase) that mention your organization or its officers.
- Periodically review traffic sources to your social media properties, as well as your website, to determine if you have visitors from unusual places or groups that oppose your organization's purpose. This may signal a potential impending problem.

Mobile Devices

At this time, there is very little anti-virus or anti-malware protection for mobile devices and smartphones. Therefore, it is recommended that you only grant mobile access to institutional systems under the supervision of an experienced service provider who clearly understands the security needs of your 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.
- If you do not have an IT department, it may be wise to assign system administrator status for all computers to one or two trusted individuals. This is especially important if you have an internal network for the sharing of files and information.
- It is a good practice to segregate general office and bookkeeping/member information to the greatest degree possible.
- Consider using a primary carrier (Comcast, Time Warner, 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 personal use of an institution's computers pose a problem, a basic "no personal use" policy is reasonable. At the very least, forbid the uploading of software that has not been cleared by your IT person.
- Downloading of any material from the Internet should be closely supervised to avoid viruses and potential copyright infringement.
- As a general rule, users should be discouraged from connecting personal devices, such as smartphones, SD cards, tablet computers and flash drives, to your institution's computer systems.

- It is also wise to conduct both tabletop and functional testing on a regular basis, with the intent of reviewing computer security response scenarios and to ensure that any software does only what it is supposed to do.
  - Tabletop drills are generally conducted as discussion-based exercises in which roles, responsibilities and response efforts for potential security incidents are reviewed. They are similar to tabletop drills you might schedule to review the same criteria for other emergency and security situations.
  - Software and website functional testing are performed on your behalf, usually by a third-party specialist, to determine if software can be used for the wrong purposes.

Passwords

- Should be at least eight characters long and contain one capital letter, one number and a symbol if possible. Use mnemonic devices to remember long passwords- example password “ipa2tfofUSoA!” is “I pledge allegiance to the flag of the United States of America!”
- Passwords should be changed every six months.

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

It 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 websites that will allow you to scan your system without charge. Try, for example,

www.grc.com or the snoop test at www.anonymizer.com. [3]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 on 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.

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

[3] 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.

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 manual 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 with law enforcement and the 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; what's important is to discuss 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 a backup copy, 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 site 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 to help offer solutions.

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.

Chapter 7

EXPLOSIVE THREAT PLANNING

Today, it's critical that every organization, regardless of size, have an explosive threat response plan (ETRP). The first step is to incorporate physical measures into your overall security plan that help prevent the planting of any device. But, since no plan is foolproof, even the most secure institution should have an ETRP as well.

Physical Security

In addition to your procedures for controlling access and preventing theft:

- Offices and desks should be kept locked, especially those that are not being used.
- Even the smallest potential hiding spaces for explosives should be identified and secured. (A device does not have to be large to cause severe physical and psychological damage.)
- Utility and janitorial closets should remain locked at all times, as should boiler rooms, mailrooms, computer areas, switchboards and elevator control rooms.
- Large trash receptacles, especially dumpsters, should be kept locked, made inaccessible to outsiders and kept far away from buildings. The areas around these items should remain free of debris.
- Cars and trucks should be required to maintain a safe, 50- to 100-foot setback from the facility. (See the section of this chapter on Car Bombs for more detailed information on parking-related security measures.)
- When planning new facilities, create as deep a setback, also known as standoff distance, as possible.
- As flying glass is a grave source of danger, consider using blast-resistant walls and

shatterproof, blast-resistant windows in your facility. Similarly, consider minimizing glass panes and coating them with shatter-resistant film.

- Shrubs, plants and trees should be trimmed, so they don't provide a hiding space for explosives and those carrying such devices.
- Employees should be encouraged to maintain tidy work areas so that they or their coworkers will notice if something unusual is present.
- As 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.
- Examine the local area to identify risks from neighboring institutions and potential targets.

Preparation

As explained in the first chapter, in any emergency firm lines of command, control and communications are essential. This is especially true when developing and implementing an ETRP. It is essential that a decision-maker be identified, that this person have the authority to act and that their decisions be effectively communicated to those who need to know them.

During the development of your ETRP, you will want to:

- Consider establishing a command center so your decision-makers immediately know where to meet during an emergency.
  - — You may wish to have building plans, contact information and other institution-specific critical information stored at this location for just such emergencies.
  - — A second, alternate site may be necessary if the first site is unsafe or unavailable.
  - — Ensure that your command center can be accessed and operated before, during and after business hours.

  - Set up your command and communications centers (primary and secondary) as soon as possible so they will be ready when needed.

- Remember that you need to plan for the possibility that a designated decision-maker may be unavailable during an emergency.
  - Make sure that a clear chain of command is established each day in light of available personnel and attendance.
  - Ensure that the people at the top of that list are so notified.
  - Based on your security plan, an office manager or leader can make this part of their daily activities.
- Identify likely targets. Produce a master target list and use it to narrow a search in light of information received during a threat.
- Determine procedures to establish search patterns and track the progress of search teams.
- Have a roster of all necessary telephone numbers and contact methods available.

Phone Threats

Calling in a threat (and it is most often a bomb threat) is an all-too-common form of harassment against institutions. It is likely that your organization will first be alerted to a threat via phone.

- Responding to such threats requires careful planning and rigorous practice by telephone switchboard personnel, receptionists and all people who receive direct calls from outside the institution.
- As with other areas of security planning, the first step in developing a response plan for a phone threat is to meet with your local police department or explosive squad. They should be able to tell you what information they will need you to acquire from the person calling in the threat.

Stay Calm and Gather Information

When a threat comes in, it's important to remain calm; especially as a calm response may help you get important information from the caller. It may also provide the person making the threat with a "human face" to the situation. In addition:

- Do not irritate or insult the caller.
- Do not slam down the receiver.
- Try to have a second person listen in on the call. It's wise to establish a signaling system among employees ahead of time so that the person being asked to listen in knows to do so without worrying or frightening others.
- Keep the caller on the line for as long as possible. Asking them to repeat information can be a useful tactic for doing so.
- Record every word spoken by the caller. The ability to record phone calls should be factored into your overall security planning.
- Take detailed notes *even if there is a recording device installed.* (Equipment failure and human error are always a possibility with such equipment.)
- Record that information in a way that is easily readable by others. ***(See the checklist in the Appendix.)***
- 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.
- Report the information to your ETRP and Security Managers immediately.
- If the caller does not provide the specific information, ask when the explosive will go off and where is it.
- 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.
- Remain available for questioning by law enforcement.

***Remember**: During a bomb threat, do not use any devices that generate radio signals, such as cell phones, walkie-talkies, etc.*

The First Decision Point

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

Evacuate immediately.

Search and evacuate as needed.

Continue normal operations.

In all three cases, law enforcement should be notified immediately. Do not conduct your own search until after the police have arrived and advised you to do so.

All things considered, prompt evacuation is likely to be the wisest choice barring some unique aspect of your facility (e.g., a hospital) that dictates otherwise. Although it will mean a loss of work time and interrupt business, immediate evacuation is, by far, the safest policy given the potential risk to human life and safety. While there is always the possibility that an evacuation will encourage copycat threats in the long run, you can reexamine your policy if you later determine that phone-in threats are being used only for harassment.

There are additional reasons to favor an immediate evacuation policy:

- You avoid having to make that same, very difficult decision under even more trying and extreme circumstances.
- While the statistical probability is that any threat is false, such threats have led to explosives being discovered.

- Your employees and constituents will appreciate your caution — and, conversely, may react badly to your institution's not evacuating immediately.
- In the absence of an evacuation, an explosive threat caller may feel ignored and choose to escalate their activities.

Evacuation Procedures

There are three key steps to managing a successful evacuation:

Notify people of the intended evacuation.

Conduct the evacuation in a safe, orderly fashion.

Follow a plan that is flexible enough to allow the evacuation to proceed if normal exits are blocked, dangerous or damaged.

Every facility and situation are different, but best practices suggest:

- Evacuation plans should account for several different scenarios and the potential blocking of normal routes out of the building or area.
- Groups should be led by someone familiar with the exit path. That person should look for obstructions and explosives while leading others to safety.
- Safe evacuation distances vary but know that, if you can see the suspicious device or vehicle, you are too close.
- If possible, 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 supermarket) will allow you to establish such a destination. 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.
- Some institutions have established more than one safe location increasingly far from their facility (one block, five blocks, 25 blocks).

- Secondary devices (explosives left outside a facility to harm evacuees) also pose a threat. At the very least, try to ensure that evacuees are moved a sufficient distance away so as to avoid secondary danger.
- Children and other persons in need of supervision and assistance may raise special evacuation concerns. They may also have special needs upon exiting a building. Consider having "to-go" bags which contain items needed for those who would face extra hardship during an extended evacuation.

Conducting a Search

After a threat is received, a search for the explosive will probably be conducted. Depending on the circumstances, with police agreement you may choose to search before evacuating the premises, or you may move people to safety before beginning to look for the explosive device.

Do not conduct your own search until after the police have arrived and advised you to do so.

A search may be done solely by internal security and staff or with the help of local police and the explosives squad. This is another instance where understanding when and how local law enforcement responds to an emergency is critical. For example, although we strongly recommend not conducting a search before police arrive, in some areas the police or explosive unit will not respond until a device is discovered. In other localities, the police may respond to a called-in credible threat, but will not search a facility without a staff member present.

Search Tips

- If it is safe to do so, have everyone check their own workspace to ensure nothing has been hidden there.
- Have more than one person search every space, even if that space is small.

- — Ideally, your primary searchers should be divided into several teams of two.
- — Teams can be made up of supervisory personnel, area occupants or specially trained searchers (like the explosives unit).
- — While supervisors and area occupants can provide a quicker search, specialty searchers make for a safer and more thorough investigation.

- If the police recommend that institution staff or volunteers do a search, a two-person search team should:

1. Enter a room or area together.
2. Carefully move to various parts of the room and listen quietly for the sound of a timing device. Since there is a great deal of noise in typical buildings, this will require concentration and focus.
3. Divide the room into four height ranges: floor to hip level, hip to chin, chin to overhead and, finally, ceilings and fixtures.
4. Start together at a single point and, standing back to back, begin to walk the circumference of the room looking for devices in the first height range (floor to hip level). Examine everything in the room, including carpeting, ducts, heaters, etc.
5. When you meet, proceed to the center of the room and search any objects and furniture.
6. Repeat steps four and five for each of the next two height range levels.
7. Check for devices that may be hidden in false or suspended ceilings, lights and building framing elements (e.g., rafters, studs).
8. Mark a room or area as searched, so there is no duplication of effort, and no area is left unexamined. Common methods for doing so are to mark the wall with tape or hang a “search complete” sign in a prominent place.

- Search the outside of your building as well. You will want to examine:
  - — Along walls, looking behind and into bushes.

  - Inside any enclosure, including planters, sheds, etc.
  - Under and into every vehicle parked close to the building. Look for a car or truck that sits heavy on its springs or otherwise seems suspicious. Identify and examine all vehicles that do not seem to belong.
- Teams and/or your general staff should be trained in these techniques.
- If you have reason to believe that unused offices and spaces may have been compromised (we previously suggested keeping them locked), you need to search them. Your command center should have keys and access cards for all areas.

Discovery

It is critical that personnel involved in explosive searching understand that they are not to touch, move or jar any objects of concern. A searcher should only look for and report suspicious objects. They should:

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

Note: Open doors or windows to minimize damage from a blast.

Car and Truck Bombs

Your best defense against these types of bombs is largely a matter of prevention and strong physical security. Extensive physical alterations and a wide and well-detailed security program are your best defense; without them, defending your organization

against truck and car bombs is very difficult. Still, there are less drastic precautions that can help mitigate the threat.

Recommendations for Securing Parking Areas

Your highest priority should be to exclude potentially dangerous vehicles from the area, but it isn't always possible to scrutinize every car or truck before it's admitted to the grounds. Examining suspicious vehicles or drivers once they are on your grounds is still a significant security measure, as is keeping vehicles far enough away from your building or office to prevent damage.

- Requiring cars and trucks to maintain at least a 50- to 100-foot setback from the facility.
- If no parking setback is possible, consider eliminating parking closest to your building or restricting parking access to staff and key leaders. Your institution may choose to issue windshield identification stickers to determine which vehicles belong and which need further scrutiny.
- Consider adding physical barricades, such as concrete Jersey barriers, between the street and your facility.
- Use gates and fences to prevent access by unauthorized persons.
- In an urban environment, where on-street parking is close to the facility, consider requesting no-parking designations from the local police department.
- Train staff and security personnel about the types and appearance of vehicles often used in bombings (see below).
- As suggested earlier, consider using blast-resistant walls and shatterproof, blast-resistant windows to block damaging effects to your premises.

Identifying Car and Truck Bombs

Searching suspicious vehicles in the advent of a bomb threat is essential. Car and truck bombs may be identified by the outward appearance of a vehicle, the behavior of the

driver and other suspicious signs. None of the following items are definite indicators of potential violence, and many are consistent with innocent behavior. However, they could be clues that something is amiss:

- The vehicle's driver parks but runs or walks away instead of entering your facility.
- The car or truck appears to be sitting very low on its springs, indicating unusual or great weight.
- The vehicle is parked illegally or too close to the building.
- The car or truck is an old model or a rental (as they are more likely to be used in a bombing).
- Be wary of any vehicle that appears to have been abandoned or has an expired or missing inspection sticker, registration or license plate.

Target Hardening

Making one's facility seem difficult to breach is called target hardening, and it is based on the proven premise that perpetrators prefer easy targets. The more difficult unauthorized access appears, the more likely a suspicious person will move on to another target or lose their nerve.

Hardening tactics include:

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

For additional information about developing and implementing ETRP security measures, see the Appendix or please visit www.threatplan.org and www.adl.org/security.

Chapter 8

ACTIVE SHOOTERS

The term "active shooter" refers to an individual actively engaged in killing or attempting to kill people in a confined and populated area. In most cases, active shooters use firearms, and there is no pattern or method to their selection of victims. While each situation and its circumstances are unique, all such events are unpredictable and evolve quickly. [4]

Immediate police intervention is the best course of action and can help mitigate harm to those under siege but, because active shooter situations often escalate and even end before law enforcement arrives on the scene, individuals must be prepared both mentally and physically to deal with the situation.

The information and recommended actions that follow reflect generally accepted practices by the U.S. Department of Homeland Security and other respected protective organizations. Your actions, of course, will also be highly influenced by the unique factors of any active shooter situation.

Regardless of the situation or specific appropriate action, notifying law enforcement is a key priority. It should occur as soon as possible.

Evacuate (Get Out)

If there is a safe way to do so, evacuate the area immediately. (See page 46.) If possible, pick the best route with opportunities for cover or concealment, and 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

[4]The guidance on active shooters in this section was prepared by ADL's National Communal Security Committee.

(so as not to confuse police) 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 by hiding. Seek shelter in an area or room where the shooter is less likely to locate you, and then take appropriate measures to lock yourself in 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 such as desks and cabinets.
- Shelter behind fire walls if available.
- Stay away from doors that can be easily shot through.
- Make a plan for protecting yourself and others should the suspect breach the door.

Call for Help (Call Out)

As soon as possible and when communication is feasible, contact 911 and provide the following information:

- Specific location including building name and office/room number.
- Number of people at your specific location.
- Number of people injured and the type of their injuries.
- Assailant(s) location, number of assailant(s) and other pertinent information:
  - Race and gender.
  - Description of their clothing and physical features.
  - Types of weapons (long gun or handgun, knives), sounds of separate explosions from gunfire, etc. and description of any bags.

- Assailant(s) identity (if known), and demeanor of the suspect —calm, agitated, angry, violent.
- Assailant(s) intentions and/or demands.

Confront the Active Shooter (Take Out)

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 option. As an absolute last resort, attempt to disrupt the active shooter by:

- Raising your voice or yelling.
- Acting aggressively.
- Committing to your actions.
- Throwing items and improvising weapons.

Public Law Enforcement Operations

The police and emergency services have protocols to follow, and it is important that you understand what those are and how you can best be of help and not interfere with their operations.

- Once on the scene, 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.
- Arriving officers usually form into groups of four to move towards or 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 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 interacting with law enforcement during an active shooter event, you will need to be cognizant of what to expect and what is expected from you:

- Keep your hands visible.
- Expect to be searched.
- Follow directions when being escorted out of the building.
- After evacuation, you may be taken to a staging or holding area for medical care, interviewing, counseling, etc.
- Once evacuated, you will not be permitted to retrieve items or access the area until law enforcement releases the crime scene or issues the "all clear" sign.

In particular, facility managers, site security or organization leaders on-site should:

- Contact the police and transfer all gathered information to them.
- Provide information on number of suspects, hostages, locations, injuries, etc. (This may have been done by an initial caller, but should be repeated or confirmed as necessary.)
- Monitor CCTV surveillance screens or footage 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 allow people inside the facility to escape.
- Initiate an active shooter announcement by utilizing an overhead paging system, instant messaging or other appropriate methods of communication. Describe the location and provide instructions.
- Direct responding law enforcement officials to the location of the incident, provide all

appropriate known information and furnish access cards, keys and floor plans.

- Deal with the aftermath. (Although every situation is unique, potential solutions should be covered in your security plan.) This includes caring for victims and their families.

(See the Appendix for more information.)

Chapter 9

EVENT SECURITY

Event security rests on the simple principle of *excluding* unwanted persons and *including* welcome ones. Failing to exclude someone who should be kept out is considerably more dangerous than blocking 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:

Assessing Risk

A number of elements go into any risk assessment. Among the most critical are:

- The existence of prior threats or incidents.
- The extent to which the event is open to the public.
- The extent to which the event is publicized.

Establishing a Perimeter

- Identify the area you want to protect (e.g., anteroom and ballroom, social hall, gymnasium or an entire building) and establish a perimeter around it.
- Identify every way in and out of that perimeter including entrances, emergency exits, kitchen doors, windows and your security screening area.
- Clear the area inside of the perimeter and inspect the entire space, looking for anything and anyone suspicious that may have been hidden before you established your perimeter.

Create a Security Screening Center

You will want to secure the area so that anyone who wants to enter must go through a checkpoint. Depending on the type of event and level of risk, that might be the place where tickets are checked, a guest list consulted or where metal detectors are deployed. Your local police department can be of assistance in determining what you need to do to keep your event secure. At the very least, everyone should be visually inspected for suspicious characteristics and behaviors.

Considerations

- 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 boundaries, guarding doors and windows, etc.
- It's important to maintain security when those responsible for the perimeter are distracted from their duties (e.g., by a medical emergency). Have a backup plan in place before the event begins.
- Guards must understand that they are securing an event, not participating in it or watching it. Therefore, they should be watching the crowd and the perimeter, not focusing on the performer, speech or activities.
- As in all things, it is critical to remember that you are bound by local, state and federal laws pertaining to discrimination and public accommodations, as well as fire codes.

Chapter 10

DEALING WITH PROTESTORS AT YOUR INSTITUTION

Even if you've never experienced a protest at your offices or property, it is important to be ready for such a situation. The following guidelines can be of help, but please remember that every protest is different and, thus, not every point below applies to every situation.

First and foremost, do not hesitate to call law enforcement if you feel threatened in any way.

Second, it is important that you refrain from engaging with the protestors or picketers.

No one should speak to or respond to them in any way, especially constituents or staff entering or leaving your facility. This can be difficult to do in the heat of the moment, but it is very important as debating with them or responding to their chants and taunts can increase the tension level and thereby increase your security risks.

Also, you may be tempted to arrange an immediate counter-protest or information-based demonstration. 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.

Make sure that your staff knows what is expected of them.

Review and Maintain Your Security Procedures

While you will want to assess the situation as it is happening and respond accordingly, it can be especially helpful to prepare your organization for the possibility of protestors. The following guidelines cover both your preparation period and/or an immediate situation.

- Ensure that your institution's rules and security procedures regarding access to your location are sufficient for the possible circumstances.
  - Make sure that your system is in place and functioning.
  - Do a double-check at the first sign of protest and be prepared to enforce your access-related rules against potential demonstrators.
  - Closely monitor who and how many people gain access to your facility.
- Beyond access control, ensure that all of your institution's security procedures are sufficient for the situation and functioning.
- Ensure that all security devices are working and being used (including door locks and alarm systems).
- Practice (rehearse) for such situations regularly.
- Ensure that unused and unmonitored entrances are closed.
- 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 related legal issues.

Contact the Police Department

- Notify the police as soon as you learn that a protest is being planned or discover it in progress.
- If you feel it's needed (and err sharply on the side of caution here), ask that officers be sent to help maintain your security.

- Understand that, where physical boundaries fall, that is where protestors may lawfully assemble near your facility or office. **Regularly check your local right-to-assemble regulations to ensure that they have not changed.**
- Notify the police if protestors on your property are acting in a threatening manner, are violent or are threatening violence. Do this even if police officers are already present at the demonstration.
- Understand permit requirements in your area, both for the protestors and for any counter-protest you may want to initiate (remember that counter-protests in the same location as active protestors is not recommended). If the protestors don't have the necessary permits, ask the police how you should proceed.
- Ask the police if they think the situation is safe enough for your normal operations or if it would be advisable to make alternative business arrangements.

Contact Your Attorney

Ask your lawyer to explain and clarify protestor rights, as well as your own. (If you don't have an attorney, you may be able to find legal assistance through the local bar association.)

- Recognize that protestors' speech and means of expression may be legally protected, especially if they are on public property. That includes but is not limited to, the distribution of flyers and other materials, chanting, holding signs and displaying photos.
- Know your own rights in a protest situation.

Consider Hiring Security Professionals

A private security professional may offer guidance and personnel for dealing with a protest. Please refer to the section of this guide that focuses on hiring outside security professionals for more information.

Prepare a Media Response

Protests are intended to attract the attention of the community, and they may draw the media. You might wish to have a representative of your organization be prepared to give a short, statement in case media representatives arrive.

- Any such statement should be written and reviewed before the interview. It can be difficult to speak extemporaneously in the height of the moment.
- Use simple, short declarative sentences.
- Develop two or three key points and stick to them.
- Make all efforts to keep the media from inviting protestors to speak during your statement.

Chapter 11

HIRING A SECURITY CONTRACTOR

As discussed earlier in this guide, your institution may decide that it's wise to bring in an outside security consultant or contractor to help with either or both security planning and implementation. Depending on the size of your organization and its specific needs, you will probably first determine whether you are best served by hiring security officers for short-term work (like events) or bringing on staff on a more permanent basis. In either case, you will want to conduct a detailed search and vetting process for your outside contractor.[5]

Short-Term Work

Should your organization find there is a need to bring in extra security for special events, holiday celebrations and larger gatherings or conferences, you will want to obtain competitive bids and begin a vetting process as quickly as possible. Local law enforcement and other organizations in your area may be able to supply recommendations. You will want to prepare a scope of work against which companies can develop their proposals and estimate costs. It should include the following:

- A concise but detailed statement describing the security tasks to be performed, including the number of days and hours that security is needed.
- A thorough set of general and particular special instructions. It is important that your organization develop these instructions; do not rely on the security contractor to provide them.
- The name and contact information of your organization's assigned liaison, who will greet security officers and ensure that they understand their role and responsibilities for each specific occasion.

[5] The information in this chapter was provided by ADL's San Diego Regional Office's Inter-Agency Security and Safety Committee.

Interacting with Security Officers

A security officers' main responsibility is to deter and detect unusual or suspicious activity as well as to safeguard property and people. Some of the key points your institution's liaison should review with an officer(s) at the start of an assignment are:

- Requirements of the assignment with an explanation of the scope of work and written expectations.
- Purpose of security during the prescribed times.
- Notice that the officer will be assessed during the shift for alertness.
- Rules of conduct that enhance effectiveness — no smoking, practical jokes, fraternization, etc.
- Contact information for the organization's liaison.
- Layout of the facility.
- Facility security and/or fire regulations.
- Location of any vulnerable areas.
- Location of telephones, fire-fighting equipment and 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 Selecting a Contractor

As soon as your organization has determined the need to hire outside security, whether on a short or a long-term basis, a contractor should be selected. The company must be reliable and in good standing, have a valid state license and meet at least the following criteria:

- Adequate and current insurance (see our website for a list of criteria).
- A strong track record and reputation:
  - Ascertain whether there has been a recent history (10 years) of valid and successful lawsuits or complaints to state agencies by consulting a lawyer or visiting your local courthouse. Request that the contractor provide "Loss Experience" or "Lose Runs" reports.
  - Consider the company's history regarding negligence, workers compensation claims and experience, and management. Ask for Employment Modification Rate (EMR) for the last three years; the lower the rate, the better the contractor's safety performance.
  - Good references.
- A security staff that is well trained and meets specific qualifications as laid out in the proposal.
- Sufficient working equipment. A cell phone is essential, and the officers may be supplied with pepper spray, batons, etc.
- A proposal that is customized based on your organization's needs. The proposal should also describe exactly how security officers will be supervised.
- Reasonable Costs:
  - Will it be a flat rate, uniform hourly rate on all employees or a unique hourly rate per individual employee? (The latter is usually the most economical.)
  - Does the proposal or contract disclose wages to be paid to security officers assigned to your site (as opposed to the rate you will be paying; so you can determine the fee/profit margin for the company)?
  - Will periodic invoices list wages and bill rates for each officer? Details should provide a good audit trail.
  - How will security pay increases be handled? Inadequate or stagnant wages lead to high turnover rates. Wages increases should be proposed in advance by the contractor.
  - Will there be additional charges made for uniforms, equipment, supplies, etc.?

- A strong documentation trail:

  The proposal should describe the type and frequency of reports and documentation such as daily officer activity logs, incident reports, crime reports, officer time sheets and other special reports.

- Good experience and management:

  Ask about longevity in the industry, especially for the company's president, regional manager and operations manager. If possible, the security contractor should have recently provided security service to an institution similar to your own.

- The proposal should include sample Post Orders or the Standard Operating Procedures Manual.

The Contract

The contract with a security contractor defines the rights and responsibilities between you and your supplier and ensures that the contractor will meet your needs. There are numerous questions and criteria that a security contract should specifically address to ensure that the firm is responsible and dependable.

- 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?
- At contract time, will there be a price increase? How much and 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 either party reasonable? (30 days is standard.)
- Is the agreement sufficiently flexible to meet your needs?
- Does it assure fairness to the contractor and adequate control to you, 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.

- Discuss your desires with the security company's management.
- Discuss the terms of supervision with the contractor, field workers and management staff. Security personnel must 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. Require that all written materials from the security officer (logs, reports, etc.) be clear, complete and usable. You should receive a copy of every report filed by your security officer.

Deciding on a Type of Security

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

After deciding what kind of security to hire, you must determine whether the security

officer(s) should be armed or unarmed. There are many costs and benefits to be considered when choosing an armed versus unarmed security officer.

The following points 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.

- Have a policy on the use of weapons with regard to deadly force. Decide whether the presence of a weapon may escalate the possible use of force and violence which otherwise might not occur**. Realize that armed officers may utilize deadly force.**
- Determine whether the members of your institution will accept an armed officer on the premises.
- Keep in mind moral questions when hiring an armed security officer.
- Determine the contractor's policy on the use of weapons with regard to deadly force.
- 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 officers, due to licensing and training requirements.
- Determine the training qualifications the security officers have with firearms.
- 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 rise of deadly force.

- The protection afforded by unarmed officers is less expensive and may incur less liability and insurance.

Chapter 12

POST-INCIDENT PROCEDURES

Whether there is trouble at an event, a protest or other emergency disturbance at your institution, your first responsibility is to handle basic life safety and emergency response procedures. The next task is to deal appropriately with the aftermath of the event, including communications, evidence protection, disaster recovery and post-incident reviews. It is wise to have outlined these procedures in your security plans and reviewed them before an event.

Command Control and Communications

As explained earlier in this guide, 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 people outside of the immediate incident, including those who need or want information, such as the media or family members of event participants. Some of these points were covered in other chapters, but you may find it helpful to have them included in this list.

- 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.
- The person designated to be your spokesperson should not have other, more important duties to attend to during an incident and recovery.
- Depending on the nature of the incident, especially if it involves children, the spokesperson might direct concerned individuals to another contact point.
- Information should be clear, factual, non-emotional and consistent with law

enforcement requirements.

Regarding the media:

- You may elect not to call them so as to minimize undue attention to the event, but their interest is sometimes inevitable. As such, plans should be made accordingly.
- The media may also be the most effective way to communicate important information to all concerned. Depending on where you are, media may be more or less receptive to becoming such a conduit. Have an alternate mode of communication identified as part of your security planning.
- Be clear, direct and honest. Speak in short, declarative sentences, like "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. In many cases, you can answer any question with these concise, stock statements:
  - "Everyone is safe; parents should call xxx-xxx-xxxx."
  - "The institution has taken appropriate security measures."
  - "A lawsuit has been filed."
- Speak to emergency officials about your message beforehand, 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, undermine attempts to determine if a subsequent incident is a copycat or 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.

Disaster Recovery

Disaster recovery is a critical part of post-incident work and, as with so many other security-related considerations, easier if preparation is done beforehand.

- Maintain current backups of critical data, vendor lists, employee information, constituent and donor contact lists and other mission-critical information off-site. Redundancy in the backup of information is recommended, as CDs or memory sticks may be damaged or destroyed, second computers or servers may go down, etc.
- Conduct an insurance review to ensure that your organization's coverage is adequate to meet all your needs. Keep insurance records with your backup information.
- Explore associated legal considerations with your institution's attorney. Discussions should include the assumption of authority, that is if someone can be granted legal authority to take emergency steps on behalf of the institution.
- Plan for relocating resident students, patients, campers, seniors and staff before disaster strikes.
- Inventory everything that would cause the institution to cease operations if destroyed.
- Review all existing service agreements as to 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.

Similarly, if threatening letters, emails or voicemails are received those pieces of evidence should also be preserved and saved so that law enforcement can evaluate the threats and determine if any crimes have been commited.

CONCLUSION

Most religious and communal institutions strive to maintain an environment that is both open and welcoming as well as safe and secure. We hope the information in this guide enables your institution to be in a better position to thwart a security emergency and to respond to a potential threat. A comprehensive security plan and strong relationships with local law enforcement will enhance your institution's ability to safely carry out your mission and work.

For additional information or more details on any of the topics covered in this guide, please visit **www.adl.org** or contact your local ADL Regional Office.

APPENDIX

HOW TO RESPOND
WHEN AN ACTIVE SHOOTER IS IN YOUR VICINITY

QUICKLY DETERMINE THE MOST REASONABLE WAY TO PROTECT YOUR OWN LIFE. CUSTOMERS AND CLIENTS ARE LIKELY TO FOLLOW THE LEAD OF EMPLOYEES AND MANAGERS DURING AN ACTIVE SHOOTER SITUATION.

1. EVACUATE
- Have an escape route and plan in mind
- Leave your belongings behind
- Keep your hands visible

2. HIDE OUT
- Hide in an area out of the active shooter's view.
- Block entry to your hiding place and lock the doors

CALL 911 WHEN IT IS SAFE TO DO SO

3. TAKE ACTION
- As a last resort and only when your life is in imminent danger.
- Attempt to incapacitate the active shooter
- Act with physical aggression and throw items at the active shooter

HOW TO RESPOND
WHEN LAW ENFORCEMENT ARRIVES ON THE SCENE

1. HOW YOU SHOULD REACT WHEN LAW ENFORCEMENT ARRIVES:
- Remain calm, and follow officers' instructions
- Immediately raise hands and spread fingers
- Keep hands visible at all times
- Avoid making quick movements toward officers such as attempting to hold on to them for safety
- Avoid pointing, screaming and/or yelling
- Do not stop to ask officers for help or direction when evacuating, just proceed in the direction from which officers are entering the premises

2. INFORMATION YOU SHOULD PROVIDE TO LAW ENFORCEMENT OR 911 OPERATOR:
- Location of the active shooter
- Number of shooters, if more than one
- Physical description of shooter/s
- Number and type of weapons held by the shooter/s
- Number of potential victims at the location

RECOGNIZING SIGNS
OF POTENTIAL WORKPLACE VIOLENCE

AN ACTIVE SHOOTER MAY BE A CURRENT OR FORMER EMPLOYEE. ALERT YOUR HUMAN RESOURCES DEPARTMENT IF YOU BELIEVE AN EMPLOYEE EXHIBITS POTENTIALLY VIOLENT BEHAVIOR. INDICATORS OF POTENTIALLY VIOLENT BEHAVIOR MAY INCLUDE ONE OR MORE OF THE FOLLOWING:

- Increased use of alcohol and/or illegal drugs
- Unexplained increase in absenteeism, and/or vague physical complaints
- Depression/Withdrawal
- Increased severe mood swings, and noticeably unstable or emotional responses
- Increasingly talks of problems at home
- Increase in unsolicited comments about violence, firearms, and other dangerous weapons and violent crimes

Contact your building management or human resources department
for more information and training on active shooter response in your workplace.

BOMB THREAT CALL PROCEDURES

Most bomb threats are received by phone. Bomb threats are serious until proven otherwise. Act quickly, but remain calm and obtain information with the checklist on the reverse of this card.

If a bomb threat is received by phone:

1. Remain calm. Keep the caller on the line for as long as possible. DO NOT HANG UP, even if the caller does.
2. Listen carefully. Be polite and show interest.
3. Try to keep the caller talking to learn more information.
4. If possible, write a note to a colleague to call the authorities or, as soon as the caller hangs up, immediately notify them yourself.
5. If your phone has a display, copy the number and/or letters on the window display.
6. Complete the Bomb Threat Checklist (reverse side) immediately. Write down as much detail as you can remember. Try to get exact words.
7. Immediately upon termination of the call, do not hang up, but from a different phone, contact FPS immediately with information and await instructions.

If a bomb threat is received by handwritten note:

- Call _____
- Handle note as minimally as possible.

If a bomb threat is received by e-mail:

- Call _____
- Do not delete the message.

Signs of a suspicious package:

- No return address
- Excessive postage
- Stains
- Strange odor
- Strange sounds
- Unexpected Delivery
- Poorly handwritten
- Misspelled Words
- Incorrect Titles
- Foreign Postage
- Restrictive Notes

DO NOT:

- Use two-way radios or cellular phone; radio signals have the potential to detonate a bomb.
- Evacuate the building until police arrive and evaluate the threat.
- Activate the fire alarm.
- Touch or move a suspicious package.

WHO TO CONTACT (select one)

- **Follow your local guidelines**
- **Federal Protective Service (FPS) Police 1-877-4-FPS-411 (1-877-437-7411)**
- **911**

BOMB THREAT CHECKLIST

Date: [redacted] **Time:** [redacted]

Time Caller Hung Up: [redacted] **Phone Number where Call Received:** [redacted]

Ask Caller:

- Where is the bomb located? (Building, Floor, Room, etc.)
- When will it go off?
- What does it look like?
- What kind of bomb is it?
- What will make it explode?
- Did you place the bomb? Yes No
- Why?
- What is your name?

Exact Words of Threat:

_____

_____

_____

_____

Information About Caller:

- Where is the caller located? (Background and level of noise)
- Estimated age:
- Is voice familiar? If so, who does it sound like?
- Other points:

Caller's Voice

Accent
Angry
Calm
Clearing throat
Coughing
Cracking voice
Crying
Deep
Deep breathing
Disguised
Distinct
Excited
Female
Laughter
Lisp
Loud
Male
Nasal
Normal
Ragged
Rapid
Raspy
Slow
Slurred
Soft
Stutter

Background Sounds:

Animal Noises
House Noises
Kitchen Noises
Street Noises
Booth
PA system
Conversation
Music
Motor
Clear
Static
Office machinery
Factory machinery
Local
Long distance

Threat Language:

Incoherent
Message read
Taped
Irrational
Profane
Well-spoken

Other Information:

_____

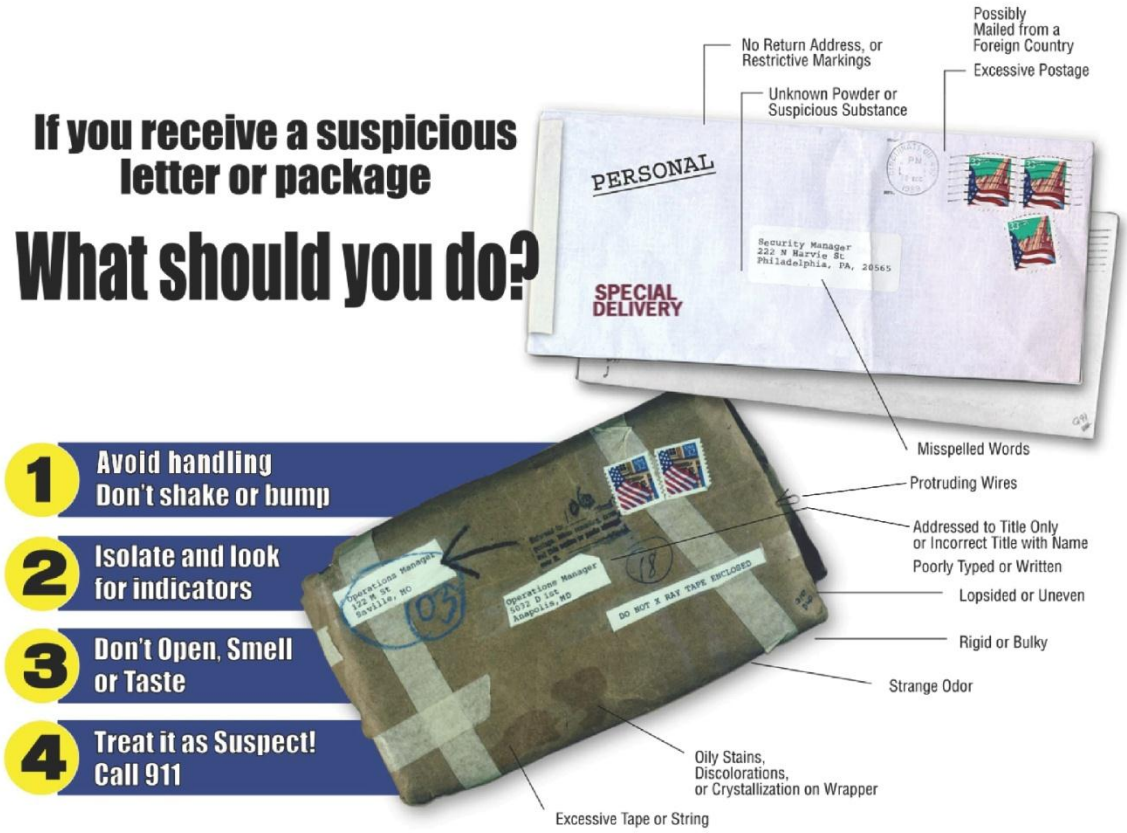
_____

Homeland Security

U.S. Department of Justice
Federal Bureau of Investigation

If you receive a suspicious letter or package

What should you do?



1. **Avoid handling** Don't shake or bump
2. **Isolate and look** for indicators
3. **Don't Open, Smell** or Taste
4. **Treat it as Suspect!** Call 911

If you suspect letter or package contains a bomb, radiological, biological, or chemical threat:

- Isolate area immediately
- Call 911
- Wash your hands with soap and water

Police Department _____

Fire Department _____

Local FBI Office _____

(Ask for the Duty Agent, Special Agent Bomb Technician, or Weapons of Mass Destruction Coordinator)

GENERAL INFORMATION BULLETIN 2000-3 (revised 5/11/2010)
Produced by: Bomb Data Center
Weapons of Mass Destruction Operations Unit

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