PM PUBLIC MANAGEMENT
April 2005 · Volume 87 · Number 3
COVER STORY

Welcome to Our (Well-Protected) Building

by Will Gunther

In an era of terror threats, workplace violence, mass shootings, and decreasing budgets, protecting staff at city and county government facilities is extremely difficult. Although technology is a great security enhancer, it is not always affordable. Not only do budgets constrain security measures, but also the need for citizens to visit government officials and use government services limits the ability to restrict access.

Procedural measures are effective security tools and are generally inexpensive. Indeed, the foundation of any good security system is effective security procedures. This article is intended to outline cost-effective ways to secure local government offices and increase visitor control, while maintaining positive relationships between citizens and their local governments.

The biggest threat to most local governments may be an attack by a disgruntled citizen or employee. The U.S. Department of Justice claims the workplace is the single most dangerous environment. In the average workplace, disgruntled former employees account for approximately 3 percent of workplace attacks. Current employees account for 20 percent of attacks, but two-thirds of all attacks are conducted by strangers. The potential for violence increases for government employees because of their daily interaction with strangers.

Procedural changes can assist in the protection of city or county staff at relatively minimal cost. The first thing to remember when developing any security procedure is that nothing good or bad happens without surveillance. Nobody will ever attack a government employee or government facility without some type of pre-attack surveillance.

Department of Justice statistics show government workers at a higher risk for violence than employees in the private sector. Government employees constitute only 18 percent of the American workforce but make up 30 percent of victims of violence. International terrorist organizations are also a threat, but harm to employees is less probable in large cities and counties like New York and Los Angeles, which are prepared to manage such attacks. Cities of this size can have large, highly trained reactive forces that decrease the potential of such attacks. Domestic terrorism is of greater concern to city or county staff than international terrorism but is still far less probable than random attacks.

Procedural changes can assist in the protection of city or county staff at relatively minimal cost. The first thing to remember when developing any security procedure is that nothing good or bad happens without surveillance. Nobody will ever attack a government employee or government facility without some type of pre-attack surveillance.

The duration and sophistication of the surveillance may vary, but there definitely will be some

type of surveillance, whether it is achieved through technology or manpower. The first place to address security and limit surveillance is in the parking lot. To be effective, security measures should work from the farthest location to the center of the facility, with its high-priority officials.

Prevent Attacks Near Buildings

Many government buildings rely on nearby parking garages for their employees, which requires workers to walk to the building either through a corridor or on the street. Particular attention should be paid to parking areas near reserved parking for government officials. Employees should be encouraged to alert security about individuals who seem to stay in their cars for too long a time, or individuals who leave the area without conducting any business in the building.

Corridor entrances should have the parking spaces near their doors reserved on all parking levels. This prevents the disgruntled citizen from parking nearby, then waiting for an official or employee to arrive and enter the building.

These spaces should be marked "reserved," but signage should not provide further information about who they are reserved for, like "City manager." This kind of designation only allows possible assailants to identify an official's vehicle with one pass through the parking garage. Officials should rotate the reserved parking spots they use.

If possible, senior officials should use government vehicles when attending such local group meetings as chamber of commerce dinners or other official functions (see box on page 12 for further individual protective measures for local government officials and employees). Employees should be escorted to their cars when they leave at odd hours.

Prevent Attacks at Building Entrances

From the parking lot, the next possible places for an assailant to observe and/or attack are the immediate access points to the building itself. All vents and maintenance access points should be secured, and a maintenance check of these places should be conducted weekly to see if anyone has tampered with them. This will ensure that no chemicals have been placed in the heating and air conditioning system or other vents that could allow contaminated air to enter the building.

This check will only take about 15 minutes out of a maintenance person's day but could pay large dividends. Even if the maintenance person isn't fully knowledgeable as to what to look for, the fact that a would-be attacker observes the vents' being checked will probably prevent such an attack.

The reception area should have a tinted-glass or one-way mirror front, except for a small portion of the divider, where the receptionist interacts with visitors. This simple, low-cost approach can create an unknown element that causes a potential attacker to search for a different building to target.

At the entrances to government administration buildings, there can, of course, be armed guards. The best way to help an armed guard to be effective is to supply an observation and reaction plan (sometimes referred to as "overwatch") to this guard because a crazed gunman or other violent attacker certainly will have developed a plan to deal with him or her. (Refer to the

box on page 13 for some details of a reaction plan.)

Because a building is meant to be accessible to the public, the guard is required to be polite and helpful and in all likelihood will never encounter a problem. Establishing observation of the guard doesn't necessarily mean paying another guard, too. Receptionists can be positioned to observe him or her. If the receptionist is not in a position to watch, an inexpensive camera can be installed to allow observation.

The receptionist should have an audible alarm to alert others of a violent attack. Avoid using a buzzer or another sound that could be mistaken for a fire alarm. If possible, a voice alert announcing something to the effect of "Danger, main entrance" would inform everyone that there is a problem and where it is, allowing security officials to move directly to the problem while informing staff to move away.

Staff members should be taught to move everyone into specific rooms if there is a problem and to lock the doors when possible, thus limiting the number of potential casualties. The audible alert will likely take the attacker out of the offensive mode and force him or her into a defensive mode because the assailant will now expect to be approached by security or law enforcement. Clearly, someone should also be designated to alert local police when the alarm is heard. The alert system itself does not have to be an elaborate and expensive system. A few loudspeakers could be enough.

In communities with a large enough budget to afford walk-through metal detectors, certain procedures should be adhered to. Often, personal effects like wallets and keys are removed from the person and handed back on the other side of the metal detectors. Handbags and briefcases also are searched, but wallets, coffee mugs, large soft-drink cups, and cigarette packs are not checked. Consider how these items are checked in your building. A medium-sized pocket knife will fit into a cigarette pack, and a small handgun will easily fit into a large coffee or soft-drink cup.

Have visitors walk through the metal detector with these items; most cups are plastic or ceramic and will not set off the detector. Wallets should receive a cursory search to make sure there are no razor blades or other potential weapons. Again, this search doesn't have to be intrusive; to an observing potential assailant, the search itself should rule out trying to hide weapons in this way.

Discovery of any form of contraband, especially contraband that is unauthorized but not illegal to possess, should require that the owner be identified. For example, a person attempts to enter with a pair of scissors in his or her briefcase. This item isn't a weapon and is legal to possess. Scissors, however, though legal to carry into the building, might well be unauthorized by the regulations for building access.

Protective Measures for Local Government Officials and Employees

Here are some measures that elected officials and staff members can use to enhance their safety:

- Senior officials should vary their exits from the office and the office parking area, when possible.

- Senior officials should drive official vehicles to functions.
- Senior officials should avoid discussing specifics about their homes or neighborhoods during parties or functions.
- All employees should vary their parking spots and be aware of the vehicle next to them, in order to easily recognize a different vehicle during evening hours.
- Supervisors and coworkers should look for signs of possible domestic violence among subordinates and coworkers; domestic violence often spills over to the workplace.
- Employees should seek parking spots in lighted areas.
- Employees should have keys in hand when approaching their vehicles, to avoid distraction in the parking lot.
- Don't use a cellphone while moving to your vehicle! It limits hearing and greatly decreases situational awareness.

The person carrying scissors most likely has no intention of using the scissors as a weapon; however, identification of the individual should be made and logged, if legal to do so. The district attorney's staff can assist in providing legal advice on this issue. Another way to check the legalities is to visit www.lawguru.com, a Web site that offers free legal advice in a question-and-answer format. The site also has a database with thousands of previously answered questions.

Such an occurrence could be an innocent mistake or simply a method of probing security measures to see what is allowed to pass. Before the 9/11 attacks, airline passengers who forgot to remove pocket knives and other forms of contraband simply turned these items over to security agents, and the items accompanied the passengers as checked baggage.

It is possible that Al Qaeda tested the airline security system with various forms of potential weapons to determine which implement had the highest success rate of passing through security procedures. We know box-cutters were the weapon of choice and were not illegal prior to 9/11. The same method of probing could happen at a government facility.

Identifying and documenting people who attempt to get into a facility with contraband will determine repeat offenders. Requesting identification and informing a person that his or her identity is being noted also may stop any further probing and force the individual to seek other targets.

Additionally, if a group wishes to continue to probe, the group will have to be greater in number to avoid repeat offenses by the same person. As groups of criminals become larger, the possibility that information about their activities will be discovered becomes greater. Inevitably, someone always has to brag about his or her exploits.

First Stop: Reception Area

The reception area should have a tinted-glass or one-way mirror front, except for a small portion of the divider, where the receptionist interacts with visitors. This prevents visitors from seeing how many personnel are in the receptionist's space, whether an armed guard is present,

if monitors are in place, and whether any other security measures are in place. This simple, low-cost approach can create an unknown element that causes a potential attacker to search for a different building to target.

Receptionists should give badges to those visitors who are going to a specific office. Badges don't have to be elaborate, just simple paper ones that are computer-generated and then laminated. They can be color-coded for certain floors and even have a letter on them to denote certain wings or sections of a building. Individuals walking in the wrong wing or on the wrong floor can be quickly identified and assisted. This measure enhances customer service while decreasing the potential for a potential attacker to be "lost" in the building while actually checking security measures. Individuals wishing to meet with senior officials should wait in the lobby until someone from the desired office comes down, greets them, and escorts them to the office.

A Reaction Plan

One way an armed guard can help provide building security is to follow an observation and reaction plan, sometimes referred to as "overwatch." Here are some suggestions for such a plan:

- One individual who can see the entrance guard should be designated to call law enforcement in the event of a confrontation. This precaution avoids the possibility that everyone will react to the immediate situation and no one will contact additional help.
- The person designated to call authorities should have a report procedure sheet on his or her desk. The report sheet should include such items as the point of confrontation (which entrance), how many attackers, what types of weapons they have, any threats or violent comments made, and vehicle description, if known. This information will assist police in immediately providing the necessary resources.
- An alarm should alert office workers to move to safe areas, avoiding the crisis area. It should alert other security officials in the building to move toward the crisis area.
- Guards who are hired to overwatch the entrance guard should be armed and trained to react to confrontation; otherwise, they are merely additional, salaried observers of impending destruction.

Receptionists should also have a stress word or phrase in the event that they are held captive and forced to call someone to the lobby. This stress word or phrase should not sound out of the ordinary, so as not to alert the attacker. The receptionist might use a specific name to address an administrative assistant in case of trouble. The name "Gertrude," for example, could be used to alert any person that there is a problem. The conversation should sound perfectly normal to the attacker: "Hi, Gertrude, this is Mary in the lobby. Could you let the deputy mayor know he has a visitor?"

Don't Lose Sight of Forgotten Visitors

Finally, such visitors as contractors installing new carpet, who employees may feel are safe just because they are working in the building, should be routed through certain stairwells or elevators. They, too, should not be allowed to wander over the building. A sexual predator who

looks the part of a contractor could easily choose a potential victim and then be able to find the victim's name, office location, potential parking spot, and vehicle over the space of a few days.

Employees begin to trust individuals they see or converse with for several days without actually knowing anything about them. Ninety-nine percent of the contractors a person ever comes in contact with are nice, trustworthy people.

A stranger you know, however, is always far more dangerous than the one you don't. Channeling the access of contractors protects them and staff. Contractors kept in one specific area can't be accused of theft or other crimes in places where they are not authorized. Once again, a simple badge worn daily would identify the area they are authorized to work in.

Behind the Scenes

Security staff should always concern themselves with all potential attack points. This includes not only the main entrance and any other pedestrian entrances but delivery entrances as well. Because loading docks and delivery entrances offer unlimited potential for the introduction of weapons or other contraband, delivery personnel should be escorted and vehicles randomly searched. It is extremely easy for a delivery person to leave a weapon hidden somewhere for future use.

In the case of a terrorist group, the weapon may be delivered for use by a staff worker inside. All food-service and other employees with access to deliveries should be subject to background checks whenever financially possible. At a minimum, food-service and other receiving areas should be checked frequently by security personnel.

Security personnel should also get into the habit of observing visitors' shoes. Shoes are the most often-overlooked item when individuals attempt to disguise themselves. A would-be attacker, for example, may dress nicely to lower suspicion when moving around the building but may have left his or her workboots on.

A person wearing a contractor's overalls may have on running shoes that are not commonplace with the normal contractor's staff. Also, contractors often bring tools and other supplies to the sites where they work. These toolboxes and other containers should be inspected daily.

Technology: Is It Worth the Money?

Many organizations invest in security cameras as part of their overall security plans. Often, however, there is too much emphasis placed on this capability. When using cameras, ensure that the personnel designated to view the monitors aren't overwhelmed by being required to watch too many monitors. Too many monitors to watch often results in none of the monitors' being observed adequately.

Security staff should be rotated through monitor stations. No one has the attention span to observe monitors for eight hours or more. Have guards change positions throughout the shift. Guards at the entrance will appreciate the overwatch of the guard in the monitor station and will be more likely to reciprocate and pay closer attention when it is their turn to monitor.

Cameras do not stop violent crime by themselves. They must be supported by security personnel able to react quickly to confrontations. And the first camera expense should be designated to the parking lot. Employees leaving work can notify the security officer in the

monitor station as to where they are parked, so the relevant camera can be watched. When possible, call buttons should be placed in the parking areas to enable employees to alert security to anything suspicious.

A public-address system in the parking area allows security officials to react immediately with a verbal warning to potential attackers that law enforcement is coming. This may be enough to save a victim during the initial stages of an attack. An attacker will immediately realize that he or she is being observed and that the escape window is closing quickly. Monitors alone will only allow law enforcement to report the type of vehicle and possible description of the attacker, but the victim still could be kidnapped or assaulted.

Though preplanned kidnappings and assaults generally take two minutes or less, a voice over a public-address system is faster than any security force in deterring them. The next place where a camera should be placed is in the main entrance, observing the entrance guard and reception area.

This article has described just a few examples of how cities and counties can protect their staff members without draining their budgets. Good security can be inconvenient, but security managers and consultants should be able to suggest cost-effective methods that have a minimal impact on the everyday functions of an organization. Obviously, larger communities have larger security budgets for some of these security measures, but the reality is that procedures are the first line of defense, and effective procedures don't have to be expensive. PM

Will Gunther is president, Operation Corporate Training (president@operationcorporatetraining.com), Newport News, Virginia (http://www.operationcorporatetraining.com).