OFFICE BUILDING SECURITY

By

Ralph Witherspoon, CPP

There are more than a million office buildings in the United States. Increasingly, more and more Americans are spending a significant part of their lives working in such buildings. Corporations and businesses increasing house their most important assets - their employees and their printed and electronic information in office buildings.

And, just like bank robbers who rob banks because that is where the money is, many criminals go to office buildings today to steal, rob, rape and spy because that is where their potential victims are located.

This brief article will provide the reader with guidance on some of the basic issues concerning securing office buildings in America today.

First, note that nothing discussed here will prevent the type of destructive attack we saw on September 11th. Only government can do that. What is addressed here is ground based attacks – both terrorist and criminal.

Both government and private commercial buildings may be targeted by terrorists. Within the US alone, the World Trade Centers (WTC) were previously targeted in 1993 with a truck bomb in the underground garage; a subsequent plot to bomb a New York City bridge and underwater tunnel was thwarted; the Murrah Federal building in Oklahoma City was destroyed in 1995 by domestic terrorists with a truck bomb; and letter bombs and anthrax letters have been sent to both government and corporate offices. The traditional threats and building security issues remain, but new (covert) terrorist threats have assumed added importance.

These terrorist threats originate not only in the international arena, but also come from a constantly changing cast of environmental, animal rights, anti-abortion, neo-nazi, anti-big business, anti-globalization, and other similar groups and activists. Some individuals in these groups have demonstrated that they are not averse to using violence to further their cause.

One Size Doesn't Fit All

Single-tenant buildings (occupied by one tenant involved in one type of business) offer different security issues and risks than does a multi-tenant / single-use building, such as a medical office building with many tenants all in the same type of business. A still different situation exists for a multi-tenant / multi-use building which may have many different tenants doing many different things, possibly including general office rental, retail operations, public utility or agency offices, operating parking facilities, and more.

How Likely a Target Are You?

There is no "cookie-cutter" plan that will secure each and every type of office building, high-rise or low-rise, and management of each will have to identify its own security needs, starting by conducting a risk assessment. How likely a target you are perceived to be by

criminals and terrorists will, in large part, determine how likely you are to be attacked. And how potential attackers perceive you depends, in part, on what visible security measures you have in place and how effective they are perceived to be.

In a commercial office building, security risks may include murder, robbery, rape, assault, theft, commercial espionage, arson, vandalism, bomb threats, and sabotage, to name but a few. The heavy concentration of people and property, coupled increasingly with "open" floor plans, make modern high-rise buildings susceptible to these type threats. Plus, the always-present life-safety risks include fire, explosion, and natural disasters. And today the possibility of a *covert* terrorist attack has to be considered by many facilities (an armed attack with multiple attackers would require police or military response).

Management responsible for securing any commercial office building should first assess the risks to the building and its tenants. A survey of all tenants should be made to ascertain what type of business each is conducting, what significant business assets are present, and which businesses, if any, may constitute an increased risk to both the building and the other tenants from criminals, political activists, political terrorists, etc.

Additionally, talking with tenants also helps get them involved in the process so that the building's security plan is not designed in a vacuum. The tenants and their employees will have to live with the resulting security plan, and if they won't cooperate with its measures, it won't work. The assessment should include a review of any known past crimes in the building along with an evaluation of crime in nearby office buildings, and in the immediate area. Local law enforcement will usually provide data on these situations.

How likely a crime target any specific building is, depends on the perceived gain to the perpetrator, balanced against his perceived risk of apprehension or defeat. For a criminal, it is usually monetary gain to be realized. For the industrial or commercial spy it is the corporate secrets and other sensitive or confidential information. For the sexual predator it is the women who work in the building or use the garage. For a terrorist it may be the media attention gained by the destruction of lives and property. This is especially true if the building is well known such as the WTC, and/or is perceived to be a symbol of America such as the Bank of America or Mall of America, or is the home of a well-known, prosperous, or controversial corporation or group such as the World Trade Organization (WTO) or the World Bank (WB).

In almost all cases the criminal will have to first access the building itself to reach his target(s). International or domestic terrorists using a bomb may only have to get "close," however, since the bomb may cause damage or causalities from a distance. Usually the criminal or terrorist prefers a "soft" or easy target, if it will achieve his objective.

Based on an assessment of the likelihood of certain security events happening, e.g. theft, assault, robbery, bombing (or damage from bomb blasts at nearby "high risk" buildings such as government buildings, etc.), a level of risk can be determined by management.

Security Survey

Next, a security survey (an exhaustive physical examination of the building, including a review of its security processes, policies and procedures) should be conducted. Local laws and codes pertaining to security measures, fire codes, and building evacuation requirements should also be reviewed. Based on the identified risks plus any identified gaps or shortcomings in security (vulnerabilities), management can start to develop an overall

security plan, and to identify cost-effective counter-measures to provide maximum deterrence to criminals and terrorists alike.

Where management does not have qualified expertise on staff, or such staff is not readily available to conduct a security survey due to other commitments, an independent, non-product affiliated security consultant should be retained to assist.

Parking and Adjacent Spaces

In most downtown office building locations management probably cannot control or prevent vehicles from stopping or parking on the public street next to their building. They may or may not be able to control the alleyways next to it. As a result, if the threat of a bombing exists, the risks from a car or truck bomb increases. Decorative concrete barriers or bollards can be used to provide some separation between vehicles and the building, thereby reducing blast effect. While the risk of bombs to most non-government or other "high-risk" office buildings is usually not high, it is not non-existent. Individual building risk may also be increased by the presence of foreign government consulates, highly visible or controversial tenants, individual federal or state government offices, etc.

Special attention should be given to any underground, adjacent, or attached parking spaces or garages. These are not only frequent targets of criminals committing theft, robbery, rape and car-jacking (and a source of many lawsuits against building owners and managers); they have also been used in some cases to place a vehicle bomb next to the building, or in a garage under the building (as in the 1993 WTC bombing).

Vehicles parking next to the building should be restricted and controlled if at all possible. If the building or its tenants are "high risk" such parking should be prohibited, or moved at least 100 feet away from the building. The destruction of the Murrah Federal Building in Oklahoma City illustrates the damage that can result from this type car or truck bomb.

If underground parking is permitted, it should only be granted to known tenants, and, depending on risk, it may be necessary that such vehicles be inspected or searched upon entry. Access of trucks to underground loading docks should be strictly controlled, with document and vehicle inspections of all trucks made prior to their entry.

Interior garage lighting should be a minimum of 5 foot-candles (55 lumens) throughout the garage, 24-hours per day. Sunlight seldom enters garage interiors and cannot be relied upon. Inspection points require at least 15-20 foot-candles (165–220 lumens) of illumination. Interior walls should be painted with a glossy or semi-glossy white paint to increase light reflection off the walls. Pillars should be painted in contrasting colors.

At stand-alone office buildings with adequate "green space" (usually in the suburbs or smaller towns) and with low traffic levels, vehicles can often be inspected (if necessary) and cleared at the entryway to the property. Speed bumps and road curves can be utilized to slow vehicle traffic, and to direct it away from the main building(s) to designated parking lots or areas.

Access Control

Because most security incidents (including most covert terrorist attacks) occur inside a building, special attention should be given to controlling building access. The nature and level of access control (along with visible security measures such as CCTV cameras) also establishes the building's security culture or "image", which is important in deterring

criminals in the first place. In cases of small office buildings, management frequently leaves the doors open for tenants and visitors. If the risks are relatively low, this may be acceptable during the office-day. Locks on exterior doors, which are closed at night and on weekends, should be of high-security commercial grade with exterior hinges "pinned."

As an alternative in buildings with only a few tenant employees, general building access might be controlled with each employee having a key or a card operating an electronic card access system. Visitors and delivery persons would have to use a building directory intercom to seek admittance. Depending on the system, tenants would then remotely "buzz" visitors in (convenient, but not very secure), or be required to physically go to the lobby or entry door to admit visitors. Building management would control building deliveries.

Where stricter access control is necessary, buildings may use a security staff (proprietary or contract guard company) to screen tenants and employees. This can be done through use of a building or tenant(s) photo ID card for visual screening by guards, or by means of one electronic card access control system for all tenants. When card access systems are used, employees/tenants can be processed automatically through one or more lines, while visitors can be directed to a special line for screening and search. Temporary (time expiring) badges could be issued to visitors who have been "approved" by tenants, or for access to "public" offices. Electronic card access control systems also have the advantage of keeping track of who's in the building, which is especially important if an evacuation becomes necessary.

Depending on risk, metal detectors to screen all persons entering for guns and knives may be appropriate in some instances. X-ray screening of packages, purses and briefcases may also be used, and is less intrusive than hand-inspecting every purse or bag.

Consideration should be given to requiring that all over-night and courier service pick-ups and deliveries be directed to a central "mailroom" or desk for appropriate screening. This prevents "delivery" or "courier" persons from roaming the building (and offices) alone and unmonitored.

Note that many large buildings require a combination of technology and manpower to adequately address their security needs. Systems and hardware won't accomplish the entire task, and neither do guards. Integrating both into a comprehensive security plan is required.

Attacking the Building

Terrorist type attacks (this could also include malicious vandalism, and major damage by disgruntled building or tenant employees) might be directed against the building itself, rather than just against the tenants and their property. Or, a building or tenant employee may use the building itself to facilitate their attack against their employer or against a single tenant. Management should secure utilities (water, power and gas) which are accessible outside, but on building property. Equal care should be given to securing access to the building ventilation system, including any access points on the individual floors.

Garbage and trash bins or skips are likely locations to hide a bomb. They should be located, whenever possible, at least 100 feet from the building, and chained or fixed to prevent their being moved back close to the building. The entire exterior base of the building (at least the first story level) should be illuminated with a minimum of one foot-candle of light. Isolated or "risk" areas such as loading or delivery docks should receive special attention, including increased lighting, locking, and observation, all to prevent unauthorized access to the

building. When a building security staff is available, CCTV may be used to monitor the exterior of the building and any associated “high risk” areas.

Bomb blasts at nearby buildings (within 4-5 blocks) may produce bomb damage by blowing out windows at your property, resulting in injury, death and property damage. While somewhat expensive, blast film over the windows can reduce or prevent injury or damage from shattered flying glass, or from glass falling to the streets below. Fixed blinds may also help reduce flying glass into the offices, although to a lesser extent.

Tenant Spaces

Due to changes in modern office building design and operation, many traditional visitor-screening methods such as elevator operators and office receptionists have virtually disappeared in many office buildings. Tenants frequently provide access control to their own spaces, sometimes with building security advice and involvement, sometimes on their own. Frequently, however, tenants don’t do much screening or control, relying instead on the building’s lobby screening (if any). As a result, thieves and Competitive Intelligence (CI) operatives (business spies) frequently have a field day.

One advantage of tenants “doing it themselves” is that where a need exists, some tenants can afford to implement higher levels of access control for their space (such as biometric access control devices) for their positive identification of their employees. This is often impracticable for large buildings as a whole. Usually this is because of the smaller numbers of employees that have to be accommodated, rather than the thousands tenants and visitors that enter a large office building daily.

Emergency Planning

Every office building, but especially high-rise (higher than 7 stories) buildings, should have an emergency plan that limits and/or mitigates the impact of any security breach or other disaster. Special attention should be given to developing and practicing building evacuation plans. While evacuation drills are inconvenient in high-rise buildings, they are critical top life-safety and should be performed at least twice a year. Warning communications are especially important and should be regularly tested (at least every 90 days). Bomb threat assessment, search, and evacuation plans should be included, and periodically tested. Building tenants and employees are less likely to panic if thy have practiced evacuations and know what to do. And lives will be saved!

Building management may require that its security officers, whether proprietary or contract, be trained in basic first aid and CPR. Security officers are often the first responders to tenant employee or visitor emergencies, especially at night and on weekends.

Periodic Review

Finally, whatever security plan is developed and implemented, it should be periodically reviewed to ensure that it is in fact operating the way it was originally designed, and that it continues to adequately address the threats to the building and its tenants which change over time, sometimes a very short time. If management does not have the in-house capability to do so, a non-product affiliated security consultant should be retained to assist with the review or audit and to provide an independent viewpoint.

Today it is not enough just to be secure, and to plan and be prepared for emergencies. In the wake of September 11th building tenants, employees and visitors are seeking a sense of

order and predictability, and must believe that they and their belongings are safe and secure.

DISCLAIMER: This article is based on generally accepted security principles, and on data gathered from what are believed to be reliable sources. This article is written for general information purposes only and is not intended to be, and should not be used as a primary source for making security decisions. Each situation is or can be unique. The author is not an attorney, is not engaged in the practice of law, and is not rendering legal advice. Readers requiring advice about specific security problems or concerns should consult directly with a security professional. The author of this article shall have no liability to any person or entity with respect to any loss, liability, or damage alleged to have been caused by the use or application of any information in this article, nor information contained on this or any linked or related web site.