

ARCHITECTURAL SECURITY: INTEGRATING SECURITY WITH DESIGN

The “form follows function” tenet of 20th century architecture holds that the specific functional requirements of a building should determine design criteria. A structure must permit efficient job performance, meet the needs of the user, and protect the user from safety hazards and criminal acts. In practice, however, the tenet is often reversed when design is focused on form rather than on function. Aesthetics, preferences for construction materials, and harmony with surroundings have predominated at the expense of the activities planned to occur within the structure.

Throughout history people have sought to control their physical environment. In the 21st century, the creation new cities and expansion of existing large cities, the further industrialization of labor, and a growth in lawlessness have led to an interest in crime prevention controls that operate at the fundamental levels of societal life. Among these is the concept of crime prevention through environmental design or CPTED.

Architects worry about the fortress mentality of security professionals while security professionals are concerned about the failure of architects to include security elements in the design of buildings from the ground up. The conflict is not over whether to include security equipment in the building design; rather, the conflict lies between a building’s openness on the one hand and the reasonable control of access to it on the other.

Making a building secure when it was not originally designed to be secure is an expensive proposition. Architects have to sacrifice much more of a building’s openness in retrofitting for security than would be the case had the building been designed for security from the outset. Protection and operating expenses are greater than they need to be because of a lack of forethought during the design of a facility. This condition is particularly evident in many of today’s buildings, where modern design and materials can result in facilities and infrastructure that are especially vulnerable.

Theoretical Background

Oscar Newman’s concept of “defensible space” focused on the vulnerability of urban housing environments to crime because of poor design. Research has shown that criminals do not move about randomly through their environment looking for a target but use a spatial search process to try to find victims or targets that match their perceptual generalizations. When a match occurs, crime is likely to occur.

Deciding to commit a crime can be seen as a process of selecting a crime target and determining a crime method by taking cues from the environment.

Paul and Pat Brantingham’s model of crime site selection is based on the following four propositions.

- Individuals who are motivated to commit specific crimes vary in character, strengths, and resources.
- The commission of an offense is the result of a multistage decision process that seeks out and identifies, within the general environment, a target or victim positioned in space and time.
- The environment emits many signals or cues about its physical, spatial, cultural, legal, and psychological characteristics.
- An individual motivated to commit a crime uses cues learned from experience and observed in the environment to locate and identify victims and targets.

Crowe, Saville, Sorenson, Atlas, and others have written extensively about CPTED and designing security into the built environment. Crime Prevention Through Environmental Design is a crime-environment theory based on the proposition that the appropriate design and application of the built and surrounding environment can improve the quality of life by deterring crime and reducing the fear of crime. Security and crime prevention practitioners should have a thorough understanding of CPTED concepts and applications in order to work more effectively with local crime prevention officers, security professionals, building design authorities, architects and design professionals, and others when designing new or renovating existing buildings.

Practical Realities

Theory holds, then, that altering the conditions that provide the opportunities for criminal behavior can curb crime. While this may be eminently sensible, great financial resources are required to alter the conditions. After a building has been constructed and put into use, the anticipated cost of physically changing it tends to overwhelm the anticipated benefits of crime reduction. Even in new construction projects, owners and investors are reluctant to commit the extra funds required to incorporate the physical features called for in the crime prevention through environmental design theory.

Reluctance to design for security is related to more than dollars. Modern buildings strive to attain openness and free-flowing movement. Design ideas that constrain and restrict are not on the agendas of the owners and not in the minds of the architects. Security features are often seen as obtrusive and lacking in aesthetic value. It seems to not matter that the world is an increasingly less safe place to work and live.

For a building to be made truly crime-resistant, security considerations must be in the architectural drawings from the very beginning. The drawings should reflect a comprehensive security perspective, one that takes into account the interrelationships between electronic security equipment, security officer services, and, most importantly, the routine and exceptional activities of the users of the building.

A common mistake, for example, is to establish an intrusion detection system without at the same time ensuring that intrusion alarms will be evaluated by a trained individual and that responses to alarms will be prompt, appropriate, and consistent with the needs of the building occupants.

We often see in facilities not designed for security a menu of problems associated with the control of human movement. These problems include vehicles backed up in and around garages and exterior entrances, employees bottle-necked at electronically controlled doors, criminal opportunists roving the stairwells in search of victims, and robberies at public service counters that were not installed with security in mind.

We also discover that electronic sensing devices do not function properly because someone failed to notice that a hanging ceiling or a wall extension would interrupt the sensing function.

The use of glass and foliage, which enhance the feeling of openness, can cause false alarms because sunlight will affect infrared detectors and motion detectors will activate when plants and trees are moved by air currents of the cooling system. Microwave detectors will react to cables moving in elevator shafts, vibration detectors will go off when the mail cart passes, and the fire department will be on the way when a cigar is lit under a smoke alarm.

False alarms cannot be taken lightly because they undermine confidence in the entire security program and they place an unnecessary burden on the response units. Also, when the false alarm rate is high, the building occupants tend to develop symptoms of the "cry wolf" syndrome and, as a result, may not react quickly and properly when an alarm is warning them of a true life-threatening condition.

In addition to the loss of life and property consequences that can flow from an improperly designed electronic system, there is the prospect of being held liable, both criminally and civilly. The governmental agencies that hold regulatory authority in matters affecting public safety are increasingly under pressure from society, generally to seek criminal prosecution when violations result in death or injury. Next, the extremely litigious nature of the security industry poses great potential loss in terms of compensatory and punitive awards and loss of reputation. A property owner or manager who makes security-sensitive design decisions without the input of a competent security professional is taking on a very large risk.

Security as a Design Requirement

Architects and designers can make the greatest contribution to meeting a project's security objectives. Architects generally make the basic design decisions about circulation, access, building materials, fenestration, and many other features that can support or thwart overall security aims.

Building clients and design professionals are not the only ones concerned about security during the design process. Many jurisdictions require a security review by the police as part of the building permit approval process, much the same as with fire safety requirements. Inspectors evaluate the plans for obvious spots where assaults, mugging, break-ins, and other crimes of opportunity may exist. Many jurisdictions have security ordinances that require certain lighting levels, and secure door and window designs and hardware. All federal government buildings must comply with the GSA Security Standards from 1995, and relates the many security classifications of government buildings.

If security is treated as one of the many design requirements, then the implementation and costs for such measures will be no more a burden to the project owners than fire safety features or landscaping requirements. The basic premise of security design is that proper design and effective use of the built

environment can lead to a reduction in the incidence and fear of crime, and to an increase in the quality of life. The environmental design approach to security recognizes the space's designated or redesignated use -- which defines the crime problem -- and develops a solution compatible with that use. Good security design enhances the effective use of the space at the same time it prevents crime.

The emphasis in security design falls on the design and use of space, a practice that deviates from the traditional. The traditional approach focuses on denying access to a crime target through physical or artificial barriers, such as locks, alarms, fences, and gates. This approach tends to overlook opportunities for natural access control and surveillance. Sometimes the natural and normal uses of the environment can replace or work in harmony with mechanical hardening and surveillance techniques. An intelligent use of the environment will present three basic strategies: access control, surveillance, and territorial reinforcement.

Access Control. This strategy embraces the tried and true custom of utilizing security guard forces, and the less understood and infrequently applied strategy of making use of terrain and spatial characteristics and natural circulation patterns. Access control can be augmented by mechanical safeguards such as locks and card key systems. The central objectives of an access control strategy are to deny access to a crime target and to create in the mind of the criminal a belief that an attack on the target will present personal risk.

Surveillance. A strategy based on surveillance is directed at detecting intrusion attempts, keeping an intruder under observation, and launching a response to an intrusion or an attempt at intrusion. A surveillance strategy can take advantage of terrain features, such as landscaping; building features, such as raised entrances; organized methods, such as patrolling; and electronic supplements, such as closed-circuit television.

Territorial Reinforcement. The thrust of this strategy is that physical design can create or extend the sphere of influence naturally exercised by the users of the territory. The idea is that an individual's sense of proprietorship concerning a place of work or domicile can be enhanced and extended by conscious individual action and by cooperating with others in a variety of crime-suppressing activities.

In a residential setting, individual actions can include installing lights, fences, locks, and alarms; cooperative actions can include neighborhood watch and patrol programs; and confronting suspect criminals who enter the neighborhood can combine individual and cooperative action. Territorial reinforcement communicates to criminals a message that they don't belong, that they are at risk of being identified, and that criminal behavior will not be tolerated by the residents.

The Architect Is the Key

The architect is the key to opening the opportunities inherent in the crime prevention through environmental design approach (CPTED). The architect is the essential element in creating a structure that will work in tandem with the various CPTED strategies. However, to be effective in this regard, the architect must be skilled in three areas.

Determining Requirements. Security needs must be determined early in the project's programming and problem-defining stage. The design team should analyze the designated purpose of how the space or building will be used. The designated purpose will be clear when designers examine the cultural, legal, and physical definitions of what the prescribed, desired, and acceptable behaviors are for that space. The space can then be designed to support desired behaviors and the intended function of the space. The design team should inquire about existing policies and practices, so that this information will be integrated in the programming process.

Knowing the Technology. Rapid and substantial advances in the technology of security systems make keeping up-to-date a challenge. Many construction projects, even those that may be seen as routine, will require the services of an architect knowledgeable in security principles and applications. An important competency is to understand and bring into existence the expressed needs of the security professionals representing a building's owner or manager. Within this competency is the ability to know when an expressed security need cannot be filled by a particular design idea and how to lead the security professional to an alternate idea.

Construction management, usually for reasons of economy, will sometimes invite an electronic security system vendor to act as an unpaid security consultant in matters involving major design decisions. The problem in such an arrangement is that the vendor's expertise will be in manufacturing and selling a product, not in providing an unbiased consulting service. The vendor's design recommendations are likely to reflect what will be best for the vendor in the short term without regard for the building occupants in the long term. Experience has shown this to be a primary reason underlying the poor performance of electronic security systems.

This is not to say that vendors should be excluded from contributing to the design, only that their contributed ideas should be critically examined by the design team for practicality and efficiency. Good sense dictates that all ideas, irrespective of source, be looked at from every perspective. The architect's best contribution to a project may be in providing a constructively critical analysis of security design concepts.

Understanding the Implications. Designs must integrate the complicated and sometimes conflicting goals of security and safety. The tendency to want to lock out the undesirables can create serious safety drawbacks in situations that require quick and unhampered egress. Space and function are variables that must also be brought into balance with security objectives.

Security and safety needs can be integrated in a five-stage approach. First is the problem statement, which explores the users' needs and leads to the development of functional requirements. Second is developing the scope of work from the problem statement, client expectations, and staff available. This stage should lead to a signed contract. Third is the design and documentation of the building and systems. It is at this stage that most architects go through schematic design, design development, and construction documents. Stage four is the administration and supervision of construction, and stage five involves acceptance testing, training, and setting up the building for occupancy.

Design Planning

Whenever possible, security planning should begin during the site selection process. The greatest opportunity for achieving a secure operation begins with locating a site that meets architectural requirements and also provides security advantages. The security analysis in site planning should begin with an assessment of conditions on-site and off-site, taking into account topography, vegetation, adjacent land uses, circulation patterns, sight lines, areas for concealment, location of utilities, and existing lighting. Other key factors for site security planning are off-site pedestrian circulation, vehicular circulation, access points for service vehicles and personnel, employee access and circulation, and visitor access and circulation. Site analysis is a starting point in security defense planning. It considers the perimeter and grounds of the facility, including walls, plantings, fences, berms, ditches, lighting, and natural topographic separations.

The next security level is the perimeter or exterior of the building. The building shell and its openings represent a crucial line of defense against intrusion and forced entry. The area being protected should be thought of as having four sides as well as a top and bottom. The principal points of entry to be considered are the windows, doors, skylights, storm sewers, roof, floor, and fire escapes. Doors are by nature among the weakest security links of a building because they inherently provide poor resistance to penetration. Attention must be paid to the door frame, latches, locks, hinges, panic hardware, the surrounding wall, and the door leaf. Window considerations for secure design include the type of glazing material, the window frame, the window hardware, and the size of the opening. The building shell itself is a security consideration for the simple reason that the type of construction will determine the level of security. Most stud walls and metal deck roof assemblies can be easily and rapidly compromised with common hand tools. Unreinforced concrete block walls can be broken quickly with a sledgehammer or by impact of a motor vehicle. The architect's challenge is to provide security that is attractive and unobtrusive, while providing balanced and effective deterrence to unauthorized access.

Finally, the architect should design for internal space protection and specific internal point security. These security features may be necessary for the areas within a facility that warrant special protection. The level of protection may be based on zones, with access to the zones limited to persons with the required level of security clearance.

Zoning

Application of the zoning concept means control of human movement. The idea is to allow employees, visitors, vendors, and others to reach their destinations without hindrance, and at the same time prevent them from entering areas where they have no business. Controlling access to each department of a building screens out undesirable visitors, reduces congestion, and helps employees spot unauthorized persons.

Zoning design goals are accomplished through the use of unrestricted zones, controlled zones, and restricted zones. Some areas of a facility should be completely unrestricted to persons entering the area during the hours of designated use. The design of unrestricted zones should encourage persons to conduct their business and leave the facility without entering controlled or restricted zones. Unrestricted zones might include lobbies, reception areas, snack bars, and public meeting rooms. Controlled zone movement requires a valid purpose for entry. Once admitted to a controlled area, persons may travel from one department to another without severe restriction. Controlled zones might include administrative offices, staff dining rooms, security offices, office working areas, and loading docks.

Restricted zones are essentially limited to designated staff. Particularly sensitive areas within restricted zones frequently require additional access control. These might contain classified records, chemicals, drugs, cash, and the like. Security zoning is a standard design feature of hospitals, jails, courthouses, laboratories, and industrial plants.

Electronic Systems

Devices intended to detect building intrusions is a major element of security design. The performance of a security device should be measured in terms of its probability of detecting an intruder, its vulnerability to intentional defeat, and its nuisance alarm rate. With this understanding, an architect can design and specify site intrusion detection devices, building penetration sensors, motion and volume sensors for key interior areas, access control systems, personnel identification systems, and security central control stations.

The architect should take steps to assure generous wiring in tamperproof conduit and to provide a backup, uninterruptible power supply system. 6

Much has changed in security technology. Today's alarm systems work differently than systems of only a few years ago. Devices, like CCTV cameras, are much smaller and less costly, making them useable and affordable in many more situations. An interesting advance is the verified or dual technology technique used with interior motion-detection systems. Infrared detectors feel the change in temperature as a target crosses a zone, while microwave or ultrasonic detectors sense motion. Both technologies must be triggered to cause an alarm.

Architecture making a difference

Security planning is aimed at preventing crime in the built environment. The architect plays a key role in the shaping of the environment and of the cues and signals that the building sends to the user and visitors. Whether the building turns out to be safe, secure, and comfortable is a factor of how well the architect understands the intended uses. However, good architecture cannot prevent all misdeeds. The crimes that a building environment can deter by natural, mechanical, and organized means are usually external. That is, crimes from outsiders breaking in, robbery, or assault. These stranger-to-stranger crimes produce the greatest fear but not the greatest economic losses.

Internal crime represents the greatest potential loss. Terrorism of the future may not be bomb attacks on buildings but theft and destruction of assets within buildings. Can architecture make a difference in preventing internal crime? Possibly, for if a living or working environment is perceived as defensible, the occupants are likely to take greater responsibility in protecting their individual and common territories. Designing the next generations of buildings and infrastructure to be resistant to criminal attacks, or acts of workplace violence, or terrorism is incumbent upon the coordination of the design professional and the security director or consultant. Our future as a society depends on the ability to live, work, or play in buildings that are safe and secure.

Randall Atlas, Ph.D, FAIA, CPP

Sources

- Anderson, D., and M.T. McGowan, Untitled. (Progressive Architecture, March, 1987).
- Atlas, Randy. 2004. Safeguarding Buildings Against Attacks from Terror and Crime with CPTED. AIA 2004 National Convention Continuing Education.
- Behrends, J., Designing for Security. (Progressive Architecture, March, 1987)
- Brantingham, P and B., A Theoretical Model of Crime Site Selection. (American Society of Criminology, Dallas, November, 1977).
- Crowe, Tim. Crime Prevention through Environmental Design 2nd Edition. National Crime Prevention Institute. Butterworth – Heinemann. 2000.
- Keller, S., Designing for Security. (Building Design and Construction, March, 1988).
- Krupat, E., and P. Kubzansky, Designing to Deter Crime. (Psychology Today, October, 1987).
- Newman, O., Defensible Space: Crime Prevention Through Urban Design. (MacMillan, New York, 1973).
- Repetto, T., Residential Crime. (Ballinger, Cambridge, 1974).
- Sorensen, Severin L., Maurizi, Sara K., and Walsh, Ellen M., Crime Prevention Through Environmental Design in Public Housing Technical Assistance and Training Workbook, 1996.
- Saville, Gregory and Gerry Cleveland.. "Introduction to 2nd Generation CPTED". *CPTED Perspectives*. Vol. 6 (2). 2003. pp. 3-7.
- Vonier, T., General Building Design Guides. (Progressive Architecture, March, 1987).
- Walters, J., Design and Deterrence. (Security Management, December, 1984).