

ATLAS SAFETY & SECURITY DESIGN, INC.

BUILDING DESIGN CAN PROVIDE DEFENSIBLE SPACE

As published in **Access Control**, Sept 1989

By Randall Atlas Ph.D., AIA

Atlas Safety & Security Design, Inc.

Miami, Florida

A middle-aged woman shopping in mid-1986 at The Miami Design Center, a mart selling interior design merchandise near downtown Miami, Florida was accosted in the middle of the afternoon by a young man while returning to her car in the mart's lot.

The victim, who sustained a broken hip and elbow during the attack, sued the Design Center for several hundred thousand dollars for not providing the proper security via access control in the underground parking lot. Although a guard was stationed on the upper level of the mart, the woman was unprotected in the garage. The victim was spotted by her attacker coming out of the elevator. Observing her from street level, the mugger proceeded below to the lot and made his attack unobstructed and unobserved.

This incident could have been prevented had the building been designed with security in mind. The fact that security is not a prime concern on the drawing table, however, has more to do with an attitude about what architecture should be, rather than the lack of available technology. In architecture's ideal world form follows function. In the real world it seems that function usually takes a backseat to form.

What Shape Control?

Any building must meet specific functional criteria that will eventually shape it. The building's work environment must permit efficient job performance, contain certain amenities, and protect the end user from harmful situations, including fire and criminal intrusion.

Throughout history people have sought to control their surroundings. In the modern industrialized world, where terrorism and crime have become commonplace, security has emerged as a high design priority.

While architects resist the fortress mentality, many security professionals believe architects take security and safety concerns too lightly. The differences in philosophies concerning building design are apparent. While there may be no shortage in security equipment, the basic design of a building is often too accessible to suit the security professional.

Security installed after the fact is expensive. Ironically, more of the open-air qualities valued by architects is usually sacrificed when security features are installed after the building is finished.

Renowned architect Oscar Newman articulated the connection between crime and the poor design of urban housing in his concept of "defensible space." Research shows that criminals survey their environment before committing a crime, finding people who appear most vulnerable both in terms of physical strengths and location.

Criminologists believe crime could be diminished by altering buildings and outside spaces that provide safe haven for criminal activity. Unfortunately it would take considerable financial outlay to make these exterior and structural alterations. Once a building is under construction it is generally too costly to change its basic structural makeup. Once the building is occupied changes are even more difficult.

Construction and design limitations require that security adapt itself to the existing physical conditions, which are not always easy to work around. Glass and free-flowing space found in many modern buildings invite intrusion. How much easier it would be to secure a building if concerns about limiting accessibility were built into the original floorplan.

Architects often view security requirements as creative limitations, apparently unaware many security detection devices are unobtrusive. While unattractive conduits, wires, and other access control devices can be kept out of sight or be made aesthetically appealing, interior design and high-visibility furnishings like desks and consoles can further help create a feeling of inaccessibility and challenge intruders without

compromising architectural integrity.

When buildings are not initially designed with security as a priority, equipment installed after the fact may not be adequate. Open service counters including cashiers stations, pharmacy counters, and payroll counters may not be fully protected even if electronic entrance devices and receptionists are present. Open service areas and spacious, unmonitored parking lots are prime examples of indefensible space.

Areas that are difficult to secure, like loading docks, mechanical areas, inventory rooms, production lines and assembly areas, may employ electronic window and door contacts and sensors. But if the building design has called for plasterboard construction for walls and ceilings, no matter how good the technology is, it may be defeated by an intruder who is able to penetrate the ceiling or wall and disconnect the apparatus.

Some of today's most advanced security technology may be totally ineffective if building materials compromise the system. Security managers realize few, if any, devices work well in all environments and are free of false alarms. Most sensors and intrusion motion detectors are susceptible to periodic false alarms.

Architects and designers have the greatest control over how secure a building will ultimately be. Decisions concerning pedestrian circulation, access control, building materials, fenestration, along with various other features are determined by architects.



But architects, designers, and developers are not the only ones concerned with building security. Many municipalities now require a security review (similar to fire inspections) by the police as part of the building permit approval process. Inspectors evaluate building venues for potential security weaknesses. They also check the adequacy of lighting and the security of doors and windows.

Security has become such a hot issue that building managers and facilities' planners would be wise to consider it just as integral a part of management and design as fire safety features or landscaping. Security and access control is important for legal reasons as much as safety concerns. Building owners and designers failing to provide secure parking lots, sufficient security lighting, protective landscaping, and security hardware are increasingly subject to lawsuits.

The traditional target-hardening approach to crime prevention employs mechanical barriers such as locks, alarms, fences, and gates. Yet there are more natural approaches to access control and surveillance. A combination of environmental design and cooperation among citizens and police can do a great deal toward curbing crime.

Design Strategies

There are three strategies for crime prevention through environmental design (CPTED). They are:

-  access control
-  natural surveillance
-  territorial reinforcement

Access Control: This includes fences, guards, locks, and computerized card entry systems. Natural strategies for access control employ spatial definition and circulation patterns, the focus of which is to deny access to and challenge unwanted visitors.

Surveillance Strategies: These include police and guard patrols, bright lighting, CCTV, windows, low landscaping, and raised entrances.

Territorial Strategies: Included among these strategies are neighborhood crime watches, perimeter sensing systems, fences, walls, and landscaping. These methods are designed to make intruders feel unsafe and unwelcome since clear boundaries make it obvious they are intruding in someone else's territory.

Security needs must be determined early. The design team must analyze how a building will be used. The space can then be designed to foster those desired activities. Security planning should begin during the site selection process. This first stage involves analyzing conditions on-site and off-site, including topography, vegetation, adjacent land use, circulation patterns, sight lines, areas for concealment, location of utilities, and existing lighting.

In addition, off-site pedestrian circulation, vehicular circulation, access points for service vehicles and personnel, employee and visitor access, and circulation areas are also of great importance at this stage.

The second stage of security planning involves the perimeter and the building's exterior. The principal points of entry that should be considered are the windows, doors, skylights, storm sewers, roof, floor, and fire escapes.

Doors and windows offer the greatest vulnerability and must be adapted to compensate for their inherent weaknesses. Door frames, latches, locks, hinges, panic hardware, the surrounding wall, and the door leaf must be part of the initial security design.

In the case of the windows, the type of glazing materials, window frame, window hardware, and the size of the opening all figure into the security design.

Even the type of construction material could have security implications. For example, most stud walls and metal deck roof assemblies can be penetrated with small hand tools in a matter of minutes. Unreinforced concrete walls can be easily broken with a sledge hammer.

The third area of security planning is internal space. In order to secure indoor space, the building may be divided into separate zones. Under this zone arrangement, access to some areas would be highly restrictive, while other zones would offer almost universal privileges.

The zone approach controls movement of employees, visitors, and vendors within the facility by varying degrees. Unrestricted areas offering free access might include lobbies, reception areas, snack bars, certain personnel and administrative offices, and public meeting rooms.

Controlled zones offering limited access might include administrative offices, staff dining rooms, security offices, office working areas, and loading docks. Controlled zones would be accessible to employees only.

The restricted zone would be a highly secure area, with access available to only a small group of employees. Restricted zones might include vaults, records departments, store rooms for chemicals or drugs, kitchens, mechanical areas, telephone equipment room, electrical equipment rooms, control rooms, laboratories, laundry rooms, sterile supply closets, and other sensitive areas.

After official traffic patterns have been established, necessary access control and screening equipment should be selected. Care must be taken that wiring for security system networks, sensors, CCTV, door and gate controls, duress alarms, and monitors are sufficient to handle the expected work load and are tamperproof. A back-up power supply is also extremely important.

There are a variety of suggestions an architect or security professional should ask when choosing a security component such as a computerized card access system, building penetration sensor, motion and volume sensor, or a weapons detection system. Does the device really detect intruders accurately? Can it be tampered with? How often does it register false alarms?

Access control and security equipment technologies are rapidly changing. CCTV cameras have become less costly and smaller. Some access control devices employ

two kinds of technologies that must be activated simultaneously. A common example would be an interior intrusion motion detector system that uses both passive infrared and microwave technologies. Both sensors must be tripped before an alarm is sounded.

Meeting the Need

Determining what security approach and access control component is right for a particular environment is difficult. The architect sometimes allows the vendor to make this decision. This may seem to be the most cost effective and expedient way to go, but many times the vendor does not fully understand the business environment. He is not aware how many people must be employed to successfully operate the system or if the staff on hand is qualified to man the equipment.

A lot of planning and money goes into making a building secure. An architect, however, cannot change human nature. Criminal acts will be perpetrated in spite of the best-laid plans.

Security and access control systems come in many varieties and different technologies, but crime is just as diverse and the criminal as resourceful. Ironically enough, violent crime people fear most is not society's most lethal threat. Stranger-to-stranger felony crimes are less common than white-collar crime.

The violence of this century may well be replaced by industrial espionage, computer pilfering, and destruction of records as the scourge of the 21st century.

Can an architect play a part in preventing white-collar crime? Not in a concrete sense, but the architect can create an environment of safety that fosters a sense of responsibility among employees and design limited and controlled access for easy accountability. Such an atmosphere may discourage unethical or disruptive behavior.

Environmental design won't eliminate crime since it fails to attack crime's roots. Architectural security design may only be responsible for shifting crime's locale.

(from Access Control, September 1989)
