ATLAS SAFETY & SECURITY DESIGN, INC.

PAY NOW...OR LATER

As published in **Security Management**, April 1990

By Randall Atlas Ph.D., AIA
Atlas Safety & Security Design, Inc.
Miami, Florida

The value of security programming and design lies in the protection of people, information, and property. Burglary, industrial espionage, rape, assault, and employee theft all drive up the cost of doing business. As crime increases, architects are being asked to consider security.

Design without security in mind can lead to litigation, expensive retrofitting with protection equipment, and the need for additional security personnel. If security is not properly planned for and installed, security equipment can undermine key design elements and building functions.

Building and business owners have always been responsible for providing adequate security for patrons and guests. New case law has established that the failure of the proprietor, the architect, and the contractor/developer to accept the responsibility for adequate security lays the foundation for lawsuits. Furthermore, litigation has become more explicit. It extends the responsibility of the proprietor to the premises' property line rather than just the area in which business is conducted.

Liability cases have also increased because owners often make security plans on their own and fail to use a professional security planner. Having a burglar alarm or security

guard does not relieve owners of liability. They must first complete a comprehensive security survey and prepare a security plan (see Michael Wiatrowski, "Are You Liable?" Security Management, July 1986, p. 34). If a security plan is conducted but not implemented, the client is subject to litigation. The importance of premises liability and security litigation is to make security a design consideration. The only reason fire safety equipment is designed into a building is because codes require it!

If the fear of litigation is not enough to scare the client into making security part of building design, maybe the additional cost in construction, security personnel, and lost time will be. Designing without security can lead to expensive, retrofitting of spaces and the hiring of additional personnel to compensate for the deficiencies. Security as an afterthought can result in exposed, unsightly alarm systems and conduits or blocked doors and windows.

In addition to personnel costs, the placement of security guards may be disruptive to operations. Guard stations that are not planned for can be awkward if they block or obstruct entranceways. Circulation patterns in the building may be disrupted, and staff and visitors may be inconvenienced by an inefficient security plan.

A recent experience of mine typifies the resistance in so many developers to designing a plan for security. I was asked to submit a proposal to do a security design for a multiuse commercial/residential project in Key Biscayne, Florida.

The developer asked for a proposal, but did not have a budget for security. Furthermore, the architectural working drawings, which were already done, had to be redone to incorporate security. Adding to the problem was the fact that construction was about to begin, so time was limited. Had the developers considered security early in the design process, a lot of problems could have been avoided.

Another problem arose when a manufacturer's representative offered to do the security design free if the developer would use his company's equipment. This suggestion might seem like an easy solution for a builder, but in the long run it may actually be more expensive. If a builder uses only one company's products and the company goes out of business, the system has to be entirely rebuilt if something breaks. Furthermore, even if the company remains in business, if the building owner is wedded to using only one brand, he or she will not be able to seek competitive bids. Security consultants are more likely to design a system using several brands of equipment because they have no vested interest in any one product.

This same developer balked at the idea of making a threat analysis. Because of his ignorance of how a security design works, he believed all one had to do to secure a building was to design and purchase alarm systems and other, related paraphernalia.

He failed to see the importance of assessing just who would be using the systems, which would affect how they would be used.

The dollars that the developer/client was resistant to pay would buy the following essential elements:

Threat analysis. The threat analysis begins by defining the nature of the crime problem. It is the client's and the security consultant's job to define who and what needs protection, the importance of each asset, the types of threats to each asset, and how those threats can be carried out.

Many clients have only a vague sense of what they need to protect and do not have a knowledge of security strategy and technology. The client may need a security specialist to discern and describe security requirements and related costs. The architect can help the client locate the right security consultant for his or her building or particular security need.

Design considerations. The overall design of the building, even without specific security devices, is part of any security plan. Design features with particular significance for security include clear sight lines of invulnerable areas; appropriate lighting levels; the siting of the building and parking lot; the configuration of the building on the site to permit surveillance by police, users of the building, and passers-by; and physical barriers, which include perimeter walls, fences, landscaping, security windows, reinforced doors, walls, and floors. All this is in addition to actual hardware, such as special locks for doors and bars on windows.

Access control is another important aspect of the original design of a building. Access control includes access to the parking lot and grounds as well as the building itself.

Access can be limited in ways other than establishing the number of access points. Zoning, for example, simply establishes the level of access for different categories of personnel. Using this plan, a building is divided into unrestricted, controlled, and restricted areas. Security officer stations, which should be built into the original design, also restrict access.

Personnel considerations. Security consultants can help evaluate threats by or to personnel. Security design may address espionage, theft, vandalism, robbery, and assaults.

Security system development. Consultants may develop specific security devices and architectural features that have only one function - to maintain security. Included in the technological grab bag are surveillance and identification equipment, intrusion

detection devices, and parking technology systems.

The search for the best security system begins with the specifier or the architect. The specifier may be the security systems consultant. The architect is able to designate the primary entrances and exits, parking garages, and loading docks with the protection of employees and property in mind. The architect can design an integrated security system that enhances a building's overall security. The security. consultant can help the architect specify generic wiring and conduit in a building so that nearly any security manufacturer can bid on and install the system. Decisions that need to be made, for example, are whether to use shielded or nonshielded wire. Conduit can be sized to accommodate current and future wiring. Junction box locations need to be thought out for placement. The architect must specify whether cameras will be high or low voltage and whether a building will be prewired for security and life-safety systems. Security areas such as vaults, control rooms, and computer rooms need to be given special consideration in specification.

Security considerations need to be a budget line item, right next to fire safety. While costs vary based on the scope of the project, an average of $1.50 per sq. ft., or 3 percent to 4 percent of the building cost, may be devoted to security systems. A qualified person should develop a security budget, define the scope of work for security features, and develop clear qualifications for system installers and consultants.

Security professionals can save developers or clients money by addressing the total security needs and reducing early obsolescence. Developers may be reluctant to pay for a consultant to program, plan, and budget since they are often concerned with the bottom line alone. But the real bottomline is that everyone loses when security is an afterthought. When the developer turns the project over to the new owners, the problems may just begin. The alarm systems and access control systems are more than bells and whistles: they protect people, property, and information.

Architects should prepare themselves for the increasing demand for security design. They must remember that an educated client is their best customer. Clients must realize that security is as important as energy conservation, handicapped access, and fire safety.

How much security is enough? It is sufficient when a balance is reached between the level and type of risk and the cost of minimizing those risks. Security can be designed and programmed in early, or it can be done on a retrofit basis.

(From **Security Management**, April 1990)