ATLAS SAFETY & SECURITY DESIGN, INC.

ARCHITECT INPUT AMONG FIRST STEPS IN DESIGN

As published in **Access Control Magazine**, June 1991

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

The renovation, addition, or new construction of your place of business may require the security professional and owner to interface with the design professional in new and challenging ways.

The security professional may be an employee of the business and responsible for many sectors of security and safety within that business. The architect or design professional will need many aspects of information from both the owner/client and the security professional to develop the architectural program and design an efficient and secure building.

The person who can provide critical information to the architect on security needs and procedures is typically the security director. If no security director exists, then a trained security professional should be hired to provide that knowledge and assistance to the company and to the architect.

In order to provide the information in a format that the architect can work with effectively, the security professional should identify the corporate assets that are vital to protect. The three most common assets to businesses are people, information, and property.

The people resource is the first and most valuable asset to be protected and to be assessed for the purpose of developing security criteria for the architect. When performing a need assessment on any of the three assets, the critical questions are:

1. Who are the users (visitors, staff, service crew, sales)?
2. What can the users do in the building (tasks, recreation)?
3. Why are the particular users there (official business, guests)?
4. When do the users arrive and leave (times, shift patterns)?
5. Where can users go inside the building (horizontal, vertical)?
6. How can the users get there (access methods, circulation)?

The security professional will need to understand the implications of each of the answers to these questions. It is recommended that a task summary be prepared to give to the architect. The security professional will then determine the security implications and the design implications.

Security & Design Implications

Taking the example of a janitorial service, the security implications might be:

- Control of after-hours access.
- Verification of cleaning employer status.
- Sign-in policy for security supervision of entry and exit.
- Key control.

These security concerns could then translate into design implications such as:

- Design of an access control system to allow staff to control entry and to log in movement.
- Placement of garbage dumpsters.
- Location of service elevator.
- Location of service doors.
- Alarm systems for offices and control room tie-in and deactivation.

These examples are just a few of the kinds of issues and concerns that need to be addressed by the architect based on the information that the security professional has gathered.

The security professional must ask the right questions to develop security criteria. The

architectural program or problem-seeking stage should incorporate the information base developed from answers to the six questions. Later the information will be passed on to the problem solution stage of architecture: the schematic drawings, design development drawings, and construction documents.

Information, Property Protection

To protect the asset of information, the critical questions that can be asked as part of the need assessment are:

1. Who has access to the information (staff, management, mail clerks)?
2. What is the information being protected (proprietary data, trade secrets, personnel records, blueprints, computer programs)?
3. Why is the information worth protecting (what physical, operational, and dollar amounts are you willing to spend)?
4. When is the information accessible or vulnerable?
5. Where is the information available or vulnerable?
6. How can the information be legitimately and illegitimately acquired or compromised?

When the security professional understands the answers to these questions, a description of the threats and proposed solutions is presented to the architect. An example of what a security professional might present to the architect is shown below.

1. **Who:** The president of the company and top management have unrestricted access to all records. The personnel record supervisor has access only to job reviews and drug test results. Mail clerks screen mail and make copies of memos. Operation managers are responsible for control of shipping and receiving. Stock persons have access to storerooms, computer disks, archives .
2. **What:** Assets of information might include personnel files, sensitive memos, trade secrets, computer software, financial records, quarterly statements, formulas, marketing plans, client information, etc.
3. **Why:** Financial records must be protected from outside intrusion. Computer software and other records that are proprietary, classified, or sensitive must also be protected from competitor espionage, for audits, and for decision making. The owner must be prepared to provide physical protection - including fire protection and back-up protection - of records, with strict access and accountability control.
4. **When:** Personnel records are available for review upon request Monday through Friday, 8 a.m. to 5 p.m. Storage rooms are available during working hours. Shipping and receiving area, available 7 a.m. to noon, Monday through Friday. Mail and copying area, available during normal working hours. Computer room

operation, 24 hours a day. Service delivery access, Saturdays and Mondays. Most vulnerable times are during shifts and after hours from threat of burglary.

5. **Where:** Information is typically stored on most management personnel desks within their computers. Data storage is on computer disks located within the computer room. Classified and sensitive archival documents are in a vault. Vulnerable areas are the computer room, loading docks, storage rooms, vault, file cabinets, top management offices, personal computers on desk tops.
6. **How:** Office information is most vulnerable to compromise by internal threats by employees stealing memos and computer information through the unobserved availability and absence of screening and access control. Outside threats are from burglars breaking in for equipment; other threats concern collusion among daytime staff, service people, and night cleaning staff.

Once the security professional has discussed the threats and vulnerability ties with the owner/client, then counter strategies can be addressed. Architectural, technological, and organizational (security staffing) responses can now be examined for practicality and cost.

Architectural design changes to reflect the security professional's concern for protection of information could be as follows:

- Exterior penetration can de kept to a minimum by making doors easily observable, controlling those doors and monitoring them for accountability. Architecturally define the main entrance for visitors and staff. Design a service entrance that is supervisable and secure. Storage rooms can be monitored by placing them where a supervisor can oversee movement.
- Design a reception desk or counter that screens visitors, vendors, and outsiders. The counter or reception desk should be designed to view all entry doors and elevators, if provided. The reception area establishes the layering of public vs. private entry into the building.
- Provide clear demarcation of VIP areas by layering access to these zones.
- Design the computer room for strict access control. Protect utility lines. Use high-security glazing for easy supervision and visibility. Centralize the computer room's building location.
- Computers can be secured and protected in work stations with anchor pads.
- The access and egress of employees must be controlled. Controlled and supervised employee egress will permit screening of packages, briefcases, purses. Staff locker area should be well lit and located in a supervised area to prevent theft and pilferage.
- Elevators should be designed to open at the supervised core areas. Special floors or VIP offices may require special elevator access control programming or dedicated elevators.

- Service delivery areas should have a separate or clearly designated roadway system that does not conflict with employee or visitor travel. The loading dock should be designed with ground loops and intercom to notify security staff that a truck is in the loading area during hours when the loading area is not being directly supervised by personnel.
- The mail room should be located in an area that allows a clear and unobstructed line of travel from the mail loading or mail delivery area. The mail room should be a secure room with monitoring of the door to provide controlled access and accountability. If security of interoffice mail is critical, pneumatic tubes can be used for delivery of letters without human intervention.
- Placement of the vault, fire safes, and record files will depend on the frequency of use. The placement and location of these assets can be as layered or as open as the client wants.

Crime prevention through environmental design, or CPTED, uses a number of architectural, technological, and operational innovations to design in security. The possibilities are fairly endless, subject only to your creativity. The most important thing to remember is that the problem-seeking process and incorporation of resulting data should be done in the early stage of programming and schematic design.

The architect can best respond to the security professional when they participate fully - and together - in the early stages.

(from Access Control Magazine, June 1991)