Design and Deterrence:

Beyond the Stereotypes

by Jonathan Walters

IT'S NOT EXACTLY THE ODD COUPLE, but it hasn't been a match made in heaven, either: Architects worried about the "bunker mentality" of security professionals, while security professionals worried about architects' failure to include security elements in the ground-up design of buildings.

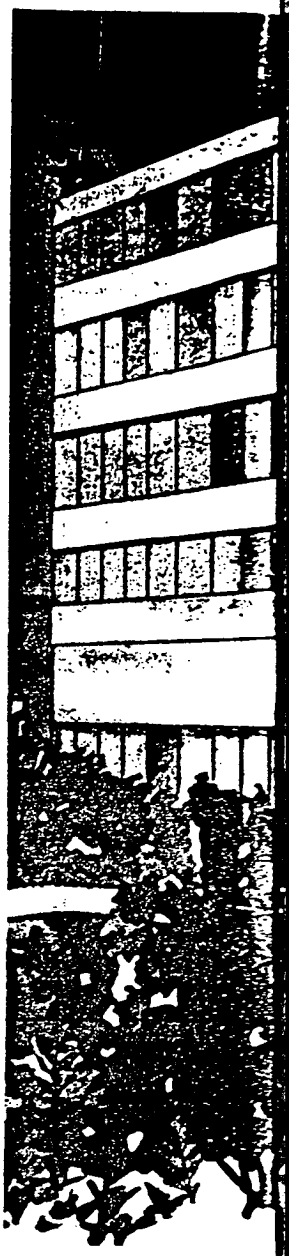
The conflict's result? Say architects, buildings that take on more of the aura of a prison than of a place to live or work. Say security professionals, buildings that may be nice to look at, but which are so riddled with security leaks neither time, money, nor prayer can plug them.

"[Design professionals] would like to see use of materials that are as appropriate as possible," says Rod Mercer, staff landscape architect with the Landscape Architecture Foundation in Washington, DC. "We'd like to get away from prominent, prison-like features in meeting security considerations."

Security professionals, on the other hand, say they would like architects to be more aware of the importance of designing security into a project. For a building to be made truly secure, security considerations must be in the blueprint from the beginning. Otherwise, you end up with a site that may have to be protected after the fact—and that can be complicated and expensive. "We're often called in after a building has been completed," says William J. Kelly, president of V.T. Technologies, Inc., a wholly owned subsidiary of Barnes Engineering Company in Stamford, CT, which specializes in design, fabrication, and installation of security systems. "Satisfying security requirements after the fact is extremely expensive—and may be nigh on impossible."

Beyond their expense and difficulty, retrofits are often controversial because they may call for significant alterations in design. This fact makes retrofits the most common battleground for architects and security professionals.

Many older foreign missions abroad offer prime examples of buildings that have undergone insensitive retrofits, according to Stuart L. Knoop, of Oudens and Knoop, a Washington, DC, architecture firm that specializes in designing US missions. Securing existing buildings has "usually involved the erection of hard defense lines insensitive to the existing architecture," says Knoop. "You see some missions where painted steel and aluminum and low-quality wood paneling are used. You often see coarsely designed, welded steel grates. Some facilities are protected by overturned flatbed trucks. And there is often a lot of poor lighting and acoustics as a result of retrofits."

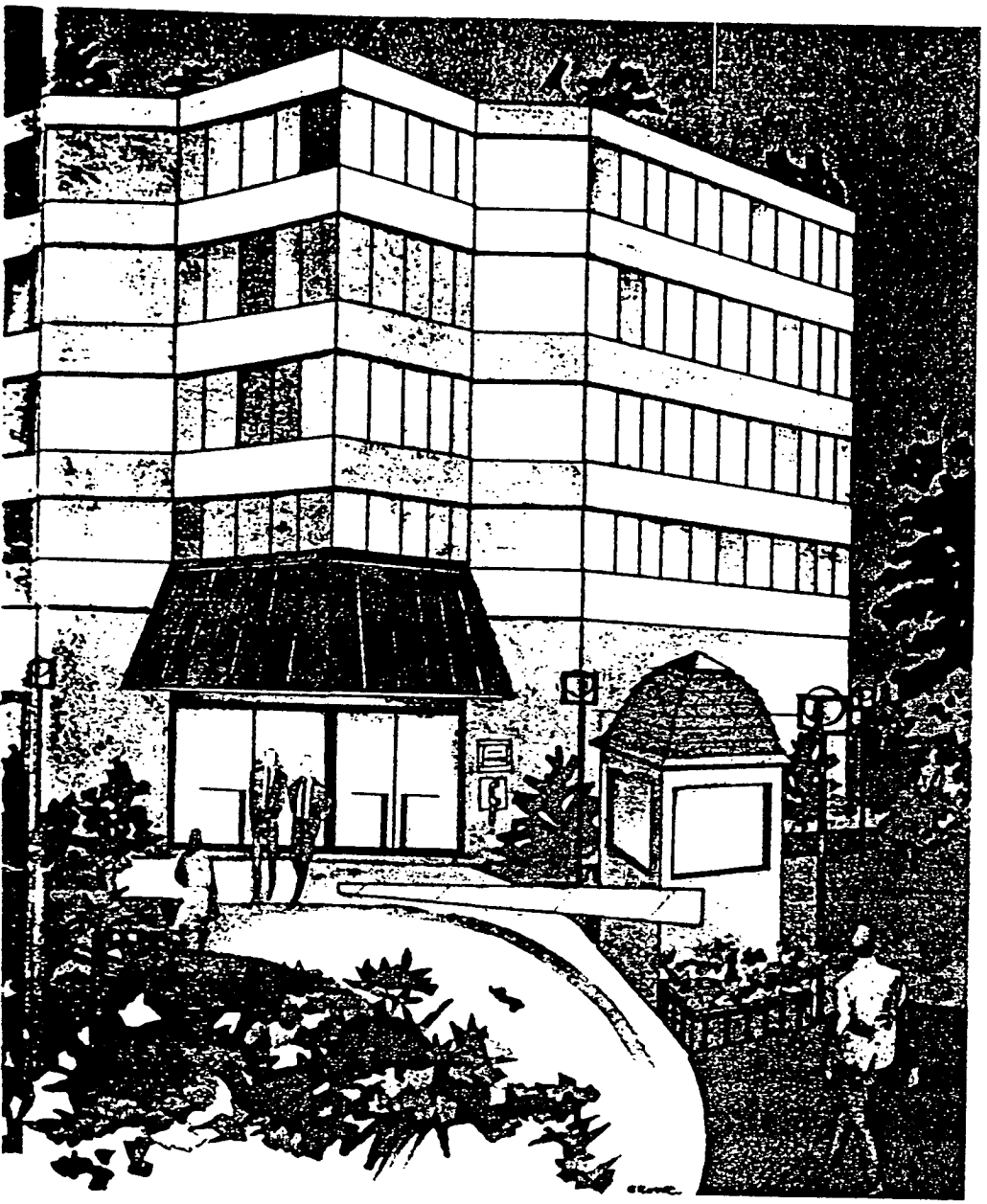


But having to come in and retrofit sensitively isn't exactly a picnic for security professionals, points out William Kelly. "Take a building with lots of nooks and crannies designed into it. If the owner later decides he wants to use CCTV cameras to monitor activity outside, you're going to need a lot of cameras." Besides the expense, he continues, "a guard can monitor one TV screen well and two poorly; three is hopeless. If the building had been designed so one camera had a clear view, you wouldn't have these problems."

With the battle lines so clearly drawn, is rapprochement possible? Absolutely, say architects and security professionals alike. What it takes is a little cooperation, a lot of communication, and a dash of mutual respect.

Cooperation is on the Rise

"Many architects are defensive about being asked to design bunkers," says Knoop. "They needn't be. The tech-



niques and technology are now available so that security doesn't have to mean a bunker." Landscape architect Rod Mercer agrees. "There are so many different plantings now, ways to use earthworks to soften the effect of fences, ways to design circulation routes for maximum security." Given today's materials and design techniques, it's possible to design security in without resorting to "prominent, prison-like features," he says.

At the same time, awareness of security considerations among architects in general appears to be on the rise. Security professionals should be used to expect increasingly fewer glazed looks when they bring the subject of security up with architects. "Until recently, I found most architectural firms viewed security as an after-the-fact consideration," says Kelly. "But that's changing rapidly."

Adds Knoop, architects who view security professionals as merely an impediment to good design have a few things to learn. "I've worked with quite a few security professionals," he says. "They know the difference between good and bad architecture."

Knoop cites work he's done at several prominent foreign missions as an example. At one where his firm worked with security specialists, a guard booth was designed and built out of the same type of marble as the building it stood by. At another site, security specialists agreed to a hard defense line pulled back from the entrance so barriers wouldn't have to be erected in the grand lobby. "They wanted a hard line that would buy them time. We gave them a design that did that," Knoop says.

Experienced architects and security professionals agree that both groups are becoming more understanding of the other's point of view. Both groups agree that retrofits put a special strain on the relationship. If security is designed into a project from the beginning, they point out, you end up with far less conflict between aesthetics and security—and you get more security at greatly reduced expense.

But working together is still a relatively new experience for architects and security professionals. Neither group is exactly sure what the other wants. They still speak slightly different languages, and they still come to a project with fairly disparate points of view. But, members of both groups believe, once each has come to understand the goals of the other, they can achieve a working relationship that is most often harmonious.

Building Function Dictates Design + Security

At the heart of harmony between architects and security professionals is one vital understanding: what the building in question is being designed to do. Understanding a building's function is vital to a good working relationship according to architects and security consultants used to working together. They share the task of designing a building that meets the client's needs.

"Is the structure to be an office building, a government building, a corporate headquarters, or what?" says landscape architect Mercer. "How will the site be used by people?" Part and parcel of these considerations, adds Knoop, is what level of security the building's function dictates. Is the client interested in preventing the theft of typewriters or in keeping employees out of the hands of terrorists?

Mobil Oil's facility in Fairfax, VA, is a perfect example of how well architects and security professionals can work together on a project, says Steve Weinberg, Mobil's manager for facilities in

Illustration by Trish Crowe

of people coming and going because the design of parking, entrances, and lobbies did not anticipate control requirements. In addition, open service counters, such as cashier, pharmacy, and payroll counters—alarmed or not—that were not initially designed to be secure, only invite robbery attempts. Inappropriate parking and pedestrian traffic patterns invite extraneous persons and congestion in critical or hazardous areas (loading dock, mechanical areas, inventory, production, or assembly), which can encourage accidents, vandalism, and theft. Electronic door and window detectors installed after the fact may be circumvented through plasterboard walls or hanging ceilings.

If the facility's security needs are addressed during its original design, the design can provide a high degree of protection and still be aesthetic and functional.

Security becomes obtrusive when it is imposed on the environment; designed into the environment, it becomes a part of the whole and far less offensive.

Components of Protection

The effective protection of any facility is accomplished through three distinct but related capabilities:

- A loss prevention management program should include identification of the types of losses to be prevented, and where and how each type of loss is most likely to occur; assignment of the responsibility to prevent loss at potential locations; acceptance of the concept that loss prevention, rather than investigation and apprehension, shall be the primary objective of the program; and identification of the methods and activities to be used to prevent each potential type of loss at all locations.
- An architectural plan should provide in its design, layout, and physical construction effective access control; and assistance to operational personnel in the prevention of loss.
- An electronic protection system, which is designed in conjunction with the architectural plan, should help achieve these objectives.

Design philosophy/loss prevention management

As with any other design specialty, security design requires a design philosophy, which has to be understood and accepted by management. For most low-security facilities, we recommend a system of loss prevention management rather than a traditional police-oriented response system. Loss prevention management uses the organization's normal management structure to identify and prevent potential loss; it is not meant to apprehend perpetrators after losses have occurred. Since the responsibility for the prevention of loss rests within the normal management structure, a facility should be designed so each department can provide for its own protection, rather than relying on a guard force. The security department and guard force should serve as a resource to line management.

The primary goals of protection design are to protect a facility and each department from penetration by persons who may deliberately or accidentally cause harm, minimize the opportunity for wrong-doing by persons properly admitted to the facility, and reduce accidents. Protection design should also give department managers an opportunity to protect and control their own departments, reduce annual protection costs, and enable each staff member to assist in the loss prevention effort by providing an environment that is easier to monitor and in which suspicious behavior becomes more evident. The final goal of a protection design plan is to provide an atmosphere of safety and tranquility.

Design techniques

The protection design goals are achieved through the following basic design techniques:

- *access control, which confines persons to certain areas of a facility where they have legitimate interests, or excludes others from a facility entirely.*
- *visibility and communication through electronic monitors, which heightens control over high-security areas.* Simple visibility of an area is insufficient; persons monitoring the area, whether in person or through electronic means, must be able to communicate with subjects in the area and detain them when necessary. A second use of the visibility technique is to place service counters, entrances to storage areas, men's and women's room doors, stairwell entrances, emergency exits, alarms, and other vulnerable spots in heavily occupied locations so they are given high visibility. Very few crimes are committed in areas containing a number of potential witnesses.
- *physical reinforcement, which should help protect entrances that are vulnerable to break-ins.* Valuable inventories, tools, pharmaceuticals, and office equipment can all entice thieves. Cashier, pharmacy, and certain other service windows should be protected with bullet-resistant glass, an emergency button or money clip, and preferably, a camera tied to the emergency button. Of course, wall construction should be consistent with the value of the contents, and these walls should extend to the ceiling slab above; hanging ceilings only provide thieves an additional entrance. Certainly, electronic devices such as movement and vibration detectors should be considered in determining what construction material to use.

Access control and the zone concept

In a zone concept, the paramount requirement is effective access control—employees, visitors, vendors, and others are assisted in efficiently reaching their destinations but prevented from entering areas where they have no purpose. Controlling access to each department screens out undesirable visitors, reduces congestion, and permits employees to identify and question unauthorized persons.

During our development of design standards for US naval medical facilities, we introduced the zone concept by segmenting the facilities into conceptual access control zones. While the specific examples below refer to hospitals, the concept is equally effective for all types of facilities.

Unrestricted zones. Some areas of a facility should be completely unrestricted to persons entering the area during hours of intended use. While steps to provide visibility/communication and site hardening may also be required in unrestricted zones, the personnel traffic load within these areas may be too great to permit effective access control.

The design of unrestricted zones should encourage persons to conduct their business and leave a facility without entering controlled areas. Hospital functions and departments that might be located in unrestricted zones include the following:

- outpatient clinic lobby
- emergency room triage, reception, and waiting areas
- main lobby, including any amenities open to all visitors, such as a gift shop, snack bar, or post office
- any meeting rooms or auditoriums that may be used by the public, persons assigned to the base, trainees, or others outside the hospital community
- dining room, if open to outpatients or the public
- personnel, purchasing, and other administration functions that frequently deal with prospective employees and vendors

Illustration by Trish Crowe

Controlled zones. While controlled areas require a valid purpose for admission, they are basically open to staff, inpatients, visitors to inpatients, and vendors. Once admitted to a controlled area, persons may travel from one department within the controlled area to another without severe restriction. Controlled areas should include the following functional areas:

- inpatient treatment areas, including inpatient entrances to clinics shared with outpatients
- administrative offices
- patient care areas
- dining room, if limited to inpatients, their visitors, and staff
- security office
- emergency command post/communications center

Restricted zones. Entrance to restricted areas is essentially limited to staff assigned to departments within that particular area. Departments within restricted zones frequently require additional access control. Functions and departments located in restricted zones should include the following:

- pharmacy preparation, where distinct from dispensing
- sterile supply, central stores, and bulk stores
- receiving and loading docks
- laundry
- food preparation, including receipt and storage
- mechanical areas and telephone, electrical, and other control rooms or closets

Some functions located in unrestricted or controlled areas may require a greater level of protection than most other functions in that area. For example, cashier's offices, pharmacies serving outpatients or emergency, radiology, silver reclamation rooms, and administrative offices containing confidential information must all have restricted access even though operational requirements may necessitate their placement in unrestricted or controlled areas. Certain other departments, such as intensive care, surgery, and laboratory, require a level of control midway between controlled and re-

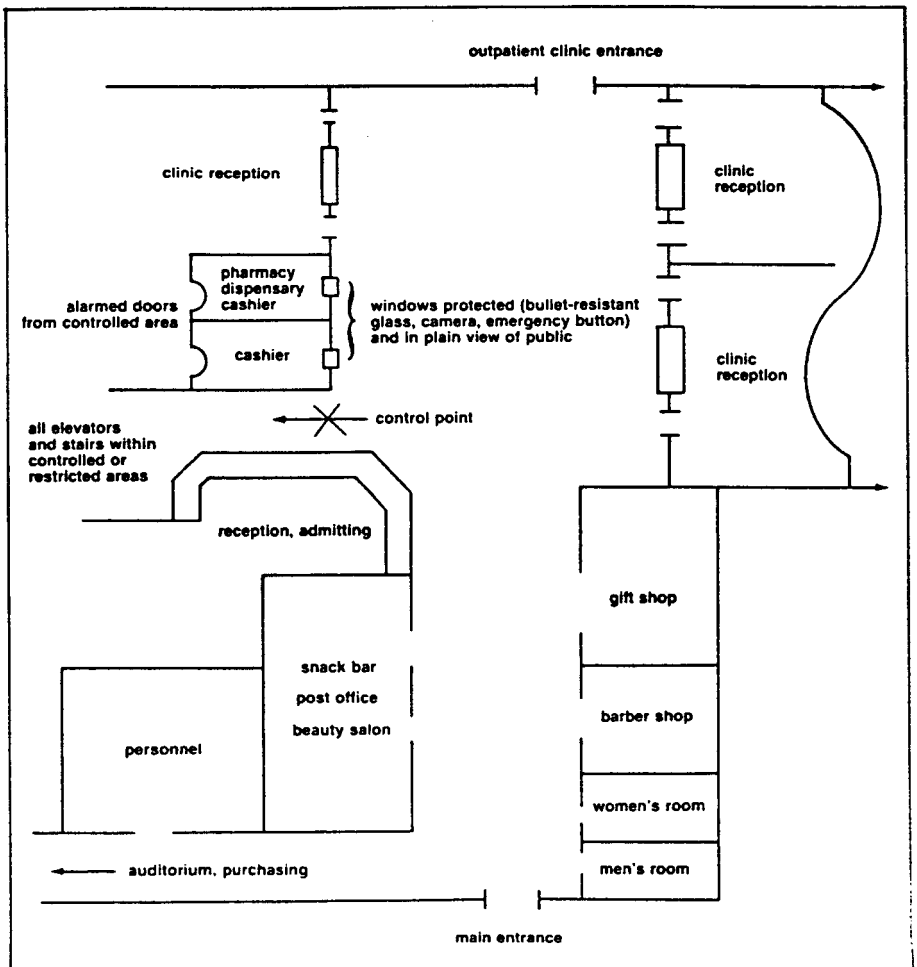


Exhibit 1—Main Entrance and Lobby

stricted. While the outpatient clinic lobby is unrestricted, entry to individual clinics would be controlled by the receptionist of each clinic.

The number of entrances between zones should be limited to the minimum consistent with efficient operations, for purposes of both visibility and access control. Fewer crossover points between zones of differing access control levels will require fewer control points. Keeping these crossover points to a minimum will reduce security operations, costly personnel, and delays for staff, patients, and visitors. Therefore, a facility should be designed with the fewest possible distinct protection zones, and each zone should contain the most possible departments requiring that level of protection.

Fortunately, this basic zone concept is being used in current efficiency designs. Progressive architects and designers have recognized the need to separate hospital facility areas that handle inpatients from outpatients and ER patients; staff from inpatient and outpatient traffic; and patients and visitors from support staff.

The protection zone concept goes beyond basic zoning to require a designer to consider security requirements when designing service modules or zones, keep the number of access points between zones to a minimum, install access controls at zone crossover points, and locate all public or semipublic functions outside controlled or restricted zones.

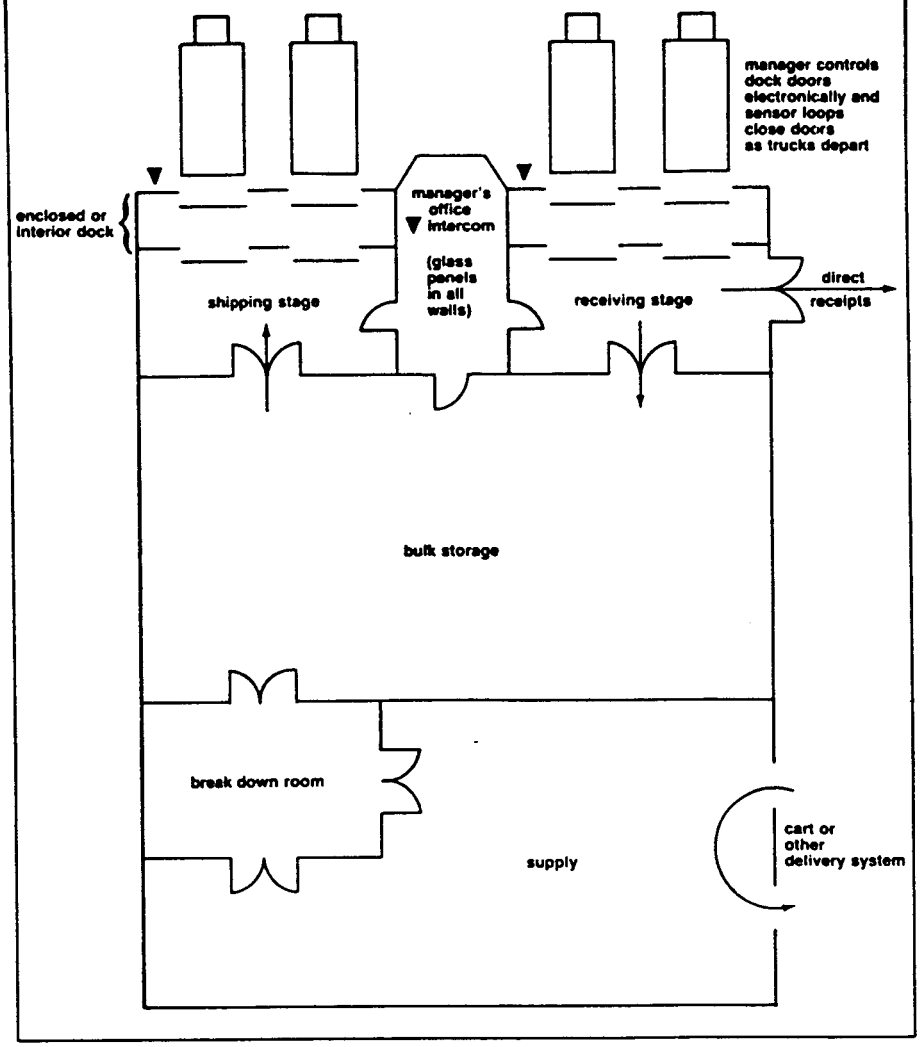
Once the zones have been identified, the designer must develop or modify parking, entrances, and personnel traffic patterns to control access efficiently. Doorways connecting less secure with more secure zones should be designed to make the most efficient use of physical design, electronic equipment, and staff. Elevators and stairwells must not provide unobserved access to controlled or restricted areas. Therefore, elevators and stairs must be located so they will service areas of equal access priority or open onto a control point. Stairs in unrestricted zones should be locked and elevator stops on restricted floors should be controlled through the use of keys or card readers.

Finally, exterior features, such as landscaping and exterior design, can be used to create a physical or psychological barrier around the facility. The more a facility is set apart from its neighborhood in terms of distance and design features, such as hedges, walls, fences, or terrain, the less likely people will casually approach it. Of course, such distancing will also estrange the neighborhood residents psychologically from the facility, which may or may not be desirable.

Exhibit 1 depicts a potential layout for the lobby of a hospital or other major facility. Entrance to the lobby is unrestricted and permits efficient use of public services. Prospective employees may visit personnel, and public groups may use the auditorium without gaining access to the rest of the facility. Of course, the auditorium may be secured when not in use, and the pharmacy and cashier's windows feature additional security measures, such as high visibility, physical reinforcement, and electronic security equipment, to discourage robbery attempts.

Exhibit 2 depicts a loading dock and

Exhibit 2—Loading Dock and Inventory Department



inventory department using the zone technique. The physical layout permits dock workers to receive, break down, and stock inventory without ever leaving the enclosed material management area. Separate shipping and receiving docks prevent the mixing of shipments and receipts. Also, the docks may be secured at lunchtime or at the end of the day. Finally, from the manager's office, a manager can see and communicate with anyone in the dock area.

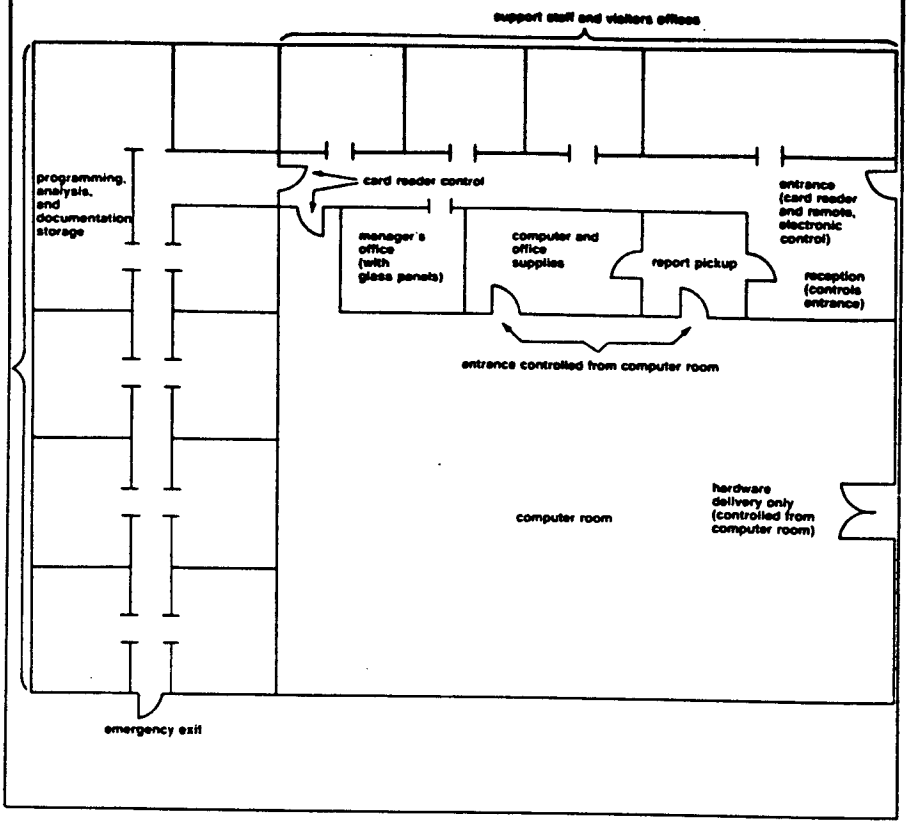
Exhibit 3 presents a data processing department design that enables data processing personnel to control access into each security level. A receptionist controls entry to the department. A card reader controls entry to the programming, analysis, and document storage areas and denies access to persons granted access to or employed in the administrative section. Also, a card reader or computer operator controls entry to the computer room. Supplies may be delivered and reports picked up without requiring access to the computer room. The computer hardware delivery door is permanently locked and alarmed, except when unlocked by the computer operator and unalarmed by the main security control officer for delivery of hardware.

During the planning stages of a new facility, it is necessary to conduct an in-depth security review in each major design phase, beginning with design concept development. Otherwise, the security measures will not be selected and implemented effectively in the architectural design. Additional time must be allocated for the design of any electronic monitoring and control systems. Several days should be allotted for architectural redesign after each security review. Construction costs will not be materially affected by the security reviews, but savings may be anticipated in the purchase of electronic controls. For instance, CCTV cameras will be used only for specific needs, rather than scattered haphazardly throughout the facility and parking lots. The design effort can also substantially reduce the need for guard forces.

Finally, the perception of a well-protected facility is a deterrent in itself. The facility whose physical design and operations communicate a sense of control and security will have a major, positive impact on employees and visitors. Thus, architectural design for loss prevention can help protect assets and people; moreover, it can help achieve operational efficiency and control costs.

Still, architects are not yet thoroughly conversant with security techniques and their application. Top management must look to both their security departments and consulting specialists to ensure these critical needs are addressed at the planning and design stages. Including loss prevention requirements in the design of facility will provide healthy savings and a loss prevention system that is compatible with the design and function of a facility. ASIS

Exhibit 3—Data Processing Department



About the Authors . . . *Robert F. Morse, II, president of Morse Consulting Company in Silver Spring, MD, has consulted to US government agencies and private industry for more than fourteen years on security hardware system design, computer design and acquisition, computer security auditing, and operational and protection management. He is a member of ASIS.*

George P. Morse, director of Morse & Associates, is an attorney. He was formerly a security officer with the CIA, and director of security for the US Public Health Service and the Department of Health, Education, and Welfare. He is also a member of ASIS.

Fairfax. The project went off without a single conflict between architect and security professional, he reports.

Why did it work so well? First, both the architect and the security consultant understood the function of the building. Furthermore, they both understood how high a priority security was for the client and how much the client was willing to spend on it.

"A security consultant has to work within a realistic budget," says Bob Hill, project architect with the St. Louis architecture firm of Hellmuth, Obata & Kassabaum (HOK), which designed the Mobil building. "Mobil was willing to go the extra mile, but most clients can't. Budget will dictate what level of security we design in."

The architect and the security professional both must understand what sort of image a client is trying to project, in the design of the building as well as the design and placement of security systems. How obtrusive do they want security to be, for example? "That might depend on how much weight the client puts on aesthetics," says Weinberg. "Or it might depend on how the client wants the people in the building to perceive security. [At Mobil's Fairfax facilities], for example, we put lots of emphasis on the employee's environment. We want it to be attractive. But at the same time, we want the employees to know they're being protected."

Once the basics have been agreed on, combining aesthetic design and security is a matter of close communication and cooperation, say the experts. Most helpful to HOK, observes Hill, was the "white paper" Mobil's security consultant put together to guide HOK's design. "He gave us a very detailed report explaining security parameters and including drawings of security points. But he did it all in layman's terms. We understood what he wanted, and we designed it in."

Even though the Mobil building was the first job HOK had worked on where security was a primary consideration, says Hill, the white paper made the job virtually routine. "Security systems are just like any other system that has to be integrated into a building," he explains. "Once you understand the client's goals and the type of hardware involved, designing it all in isn't much of a problem."

Having their own in-house electrical engineer at HOK was also tremendously helpful, says Hill. It gave the firm somebody who understood systems theory and how to integrate it with design.

Also important were the monthly meetings between the architect and security consultant that continued through both the design and construction phases of building, says Weinberg. "Communication has to be ongoing." Included in these regular discussions were Mobil staff members involved in the operation and maintenance of the security systems. Their participation, Weinberg observes, helped ensure the systems would be easy to use and simple to maintain.

A particularly sticky design-versus-security problem at Mobil's facility was the high-speed electronic key checkpoints through which all employees and visitors must pass when entering the building's offices. The trick was designing a "cattle chute" that didn't look like a cattle chute. Working with available hardware, HOK came up with a design that softens the effect considerably through the use of subtle colors and glass.

Fire exits are often another sticking point between architects and security professionals. Codes require them, but security professionals see them—rightfully so—as another hole to be plugged. But again, says Weinberg, with a little work and cooperation, such details don't have to cause trouble. "It is up to the architect to design a space that meets both safety and security requirements." In the case of Mobil, a slightly more sophisticated—and completely unobtrusive—monitoring system was developed to cover the fire exits.

The solution of the checkpoint and fire exit problems at Mobil, says Weinberg, are perfect examples of how the architect/security professional relationship should work. "The security professional tells the architect what he needs; the architect comes in with a design to satisfy that need. Then we all sit down and talk. There really shouldn't be a problem."

"I can't think of any conflict that arose," adds Hill. "We had a very clear understanding of what it was Mobil wanted, we gave them a design that fit their needs." Included in that design are 3,500 separate checkpoints in the million-and-a-half square feet of office space, including high-speed electronic card readers, video cameras and recording equipment, electronic eyes, magnetic door monitors, duress switches, radios and sound recording equipment, and x-ray equipment.

The Part Building Owners Play

Another major reason for the harmony between architect and security professional on the Mobil job was that Mobil executives insisted security be a primary element of their office building's design. But many times, architects and security professionals agree, building owners fail to see the importance of designing security into their projects. Instead, they view security as an excess, unnecessary expense.

"Even if an architect brings security up with a client, he or she is often poohpoohed," says Bruce C. Ream, executive vice president of the Correctional Housing Corporation in Chicago and chairman of the American Institute of Architects' committee on architecture for justice. "Frequently owners are not aware of the need for security until after they move into a building. Then they bring in the security professional, and the architect ends up the scapegoat." Stuart Knoop also points out that when architects bring up the question of security, building owners may view the suggestion as a ploy to increase billable hours, rather than a way to cut the client's costs in the long run.

For those clients who need to be made aware of security considerations and the cost-effectiveness of planning them in, Bruce Ream recommends that architects take clients to seminars on security. But such sessions aren't all that easy to find, says William Kelly. Education is a real problem area, he elaborates, "there is a tremendous need for [architects and security professionals] to get together to conduct seminars. Their respective organizations' annual meetings would be a perfect opportunity." In the meantime, Kelly suggests security professionals scour security-oriented newsletters and magazines for mention of such seminars.

Architect Knoop agrees that seminars that cover the architect/security relationship are tough to come by. The American Institute of Architects, he says, has showed little interest in organizing any. For the time being, this puts a great deal of the responsibility for educating building owners on individual security professionals.

If it's any comfort, says Knoop, if you can get an owner's ear, he or she is usually responsive. "Once you explain to a client how much easier it is to design security in the first place, they come around pretty quickly."

Experts find, too, that making clients aware of security issues is becoming less of a problem. Bob Hill reports that virtually every corporate client now coming

into HOK lists security as a design priority.

To respond to this demand, more and more major construction and engineering companies are forming "security groups," according to Bill Kelly. They bring an architect on board to bid and work on major construction projects involving security elements, such as corporate headquarters, utility plants, and other high-security installations.

Finding the Right Architect

Along with increasing client awareness of security, says Weinberg, should come the understanding that the security professional will be involved with the team that selects the architect for a project. Assuming it has been established that security systems should be designed in at the same time as sprinkler systems, how can a security professional find an architect to work with?

"Look at jobs similar to the one you're working on," says Knoop. "Find out who the architect was, and ask the security professional on the job how easy the firm was to work with. A lot of it is simply grapevine work." Since working on Mobil's facility, for example, HOK has had a raft of requests for corporate headquarters integrating a high degree of security.

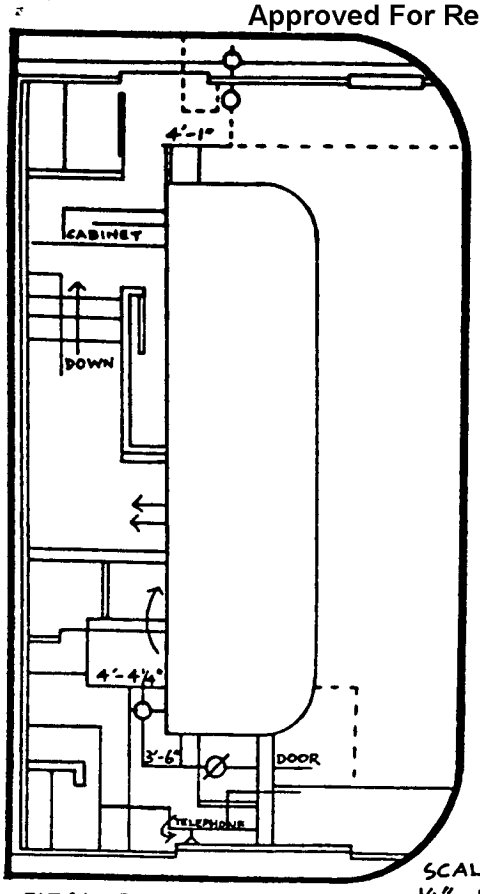
Whether a firm has its own engineering staff, both electrical and mechanical, is also an important consideration, observes architect Ream. A lack of in-house engineering expertise shouldn't disqualify an architect, he says, but the firm better have access to an experienced engineer or to a larger architectural firm that does.

Kelly says his firm is also getting entrepreneurial in its approach: he sees a lucrative future for cooperative efforts. His firm is learning about major projects that will require high-security equipment, then going out and finding architects they can work with to collaborate on such projects.

Finding architects versed in security—or willing to become versed—hasn't been hard, says Kelly, especially in an era when security is becoming a concern for everybody. "Approaching them can be tough at first," Kelly says. "But if you call and explain that they can generate more business if they consider security in design, believe me, they listen."

ASIS

About the Author . . . *Jonathan Walters is a freelance writer based in Washington, DC.*



FIRST FLOOR

Working Hand in Hand

Design & Deterrence

BY ROBERT F. MORSE II, CMC, AND GEORGE P. MORSE, JD

ARCHITECTS AND OTHER DESIGNERS take well-deserved pride in their ability to develop facilities that provide effective operations and aesthetic satisfaction, while maximizing the contribution of new technologies and minimizing support costs. For example, as personnel services costs escalated during the 1950s and 1960s, design and construction techniques were developed with minimal maintenance, cleaning, and other personnel service requirements. Similarly, during the energy crisis in the 1970s, the design community responded with energy-efficient designs and construction methods. Finally, as new management and operational methods along with more sophisticated electronic systems are being developed in the 1980s, architectural designs are being modified to incorporate and support them.

However, despite escalating threats of crime, accidents, and other hazards to all types of organizations (and the growth in available security technology, equipment, and systems), designers have virtually ignored most facilities' security requirements. The only loss prevention specialty that has been effectively addressed by designers is fire prevention.

In 1979, George P. Morse & Associates was engaged by the US Navy Civil Engineering Laboratory to investigate the protection and loss prevention concepts being incorporated into the planning, design, and construction of naval and other hospitals. The company was also asked to develop a manual of architectural techniques for protection and loss prevention. These design techniques were later incorporated, in their entirety, into the naval hospital design requirements. Following this effort, Morse & Associates was responsible for protection and loss prevention design of the new naval hospital in San Diego, CA.

During our investigation of existing hospital designs, we sent questionnaires to the designers of twenty-three hospitals. We discovered protection and loss prevention techniques were not being incorporated into the architectural design by any of the designers, other than for such basic features as masonry walls and vaults for pharmacies and certain stores. In subsequent seminars and discussions with designers of other facilities, we learned that—with the exception of jails and other high-security buildings—architectural design for loss prevention is virtually non-existent. Since a client contracting with an architectural firm does not normally think to specify protection or security in the design criteria, the architectural or engineering firm does not address it. This can only be corrected by educating builders and architects about the importance of security and security techniques.

Today, crimes against business are at an all-time high. Acts of violence, arson, thievery, drug use, and vandalism occur daily in offices, production facilities, schools, and hospitals. All the evidence points to a greater frequency, variety, and magnitude of such aberrant behavior. Moreover, security design must anticipate mores and behavior, not in terms of the climate of this or next year, but of 1990 and beyond.

Yet, facilities are still being designed as if we lived in a utopian world, where assault, carelessness, accident, waste, vandalism, and theft do not occur. Then, when these problems do occur in a facility constructed without security designed into the building, more expensive and ineffective responses ensue. Security equipment designers are expected to select and specify equipment that will not only protect the facility, but also compensate for an architectural design that, at best, offers no assistance and, at worst, compounds the hazards. It is simply unacceptable to ignore protection requirements during physical design and then rely on electronic systems and guards.

If security has not been designed into a building from the start, security, of necessity, comes to rely too heavily on CCTV systems, with cameras monitoring every area of concern. Where CCTV is installed without a compatible physical design, CCTV observers cannot distinguish proper from improper behavior, communicate with or otherwise interact with subjects, or respond with sufficient speed. (In addition, a person can only be expected to observe a CCTV monitor effectively for fifteen to twenty minutes at a time.)

In facilities that were not planned with security in mind, receptionists and electronic entrance controls are frequently overwhelmed by the number and variety