Architect as Nexus

ARCHI·TECH

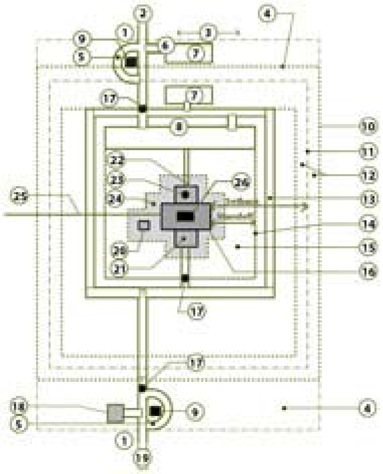
Cost-effective – and effective – security begins in design

By Dan Daley

The federal government may fail to provide a lot of things, but it never fails to offer examples of what not to do. When it comes to the confluence of security and architecture, a perfect instance is found in a General Services Administration report to Congress regarding security enhancements to federal office buildings. Between 1995, when the Alfred P. Murrah Federal Building in Oklahoma City was bombed, and 1998, when the report was made, there were 7,000 individual security enhancements requested and performed by federal agencies nationally, at a cost of $353 million. Had the security features been implemented as part of the original design, the GS's report concluded, the cost would have been a fraction of that, and the incident that sparked the round of upgrades itself might have been avoided.

Architects need to be a lot of things these days, and the role of security expert might be asking too much. But it is necessary to understand how contemporary security systems integrate with architectural design and construction. Or, at least, how they should integrate.

"The system design tends to be regarded as secondary to the architectural design," comments David Stone, president of David Stone & Associates, a Pembroke Pines, FL, building technology consultant and systems design/install company. If you don't address the security technology concerns in the initial architectural programming phase, you'll have to later, and at greater cost. As a



SOURCE: RTKL; REPRINTED FROM BUILDING SECURITY HANDBOOK FOR ARCHITECTURAL PLANNING AND DESIGN BY BARBARA A. NADEL, FAIA © 2004 THE MCGRAW-HILL COS. INC.

Click Here for Related Products

Defining The Roles

Randy Atlas, Ph.D., a registered architect, certified protection specialist (CPP), and vice president of Atlas Safety &

percentage of the overall cost of the building, that's the most cost-effective point at which to do it.

Architects are the nexus of security implementation. "Architects and designers can make the greatest contribution to meeting a projects security objectives," says Randy Atlas, Ph.D., a registered architect, certified protection specialist (CPP), and vice president of Atlas Safety & Security Design, Miami, FL. "Architects generally make the basic design decisions about circulation patterns, access control, building materials, fenestration, and many other features that can support or thwart overall security aims."

Assessing Security Needs

Integrating security into new construction has several key steps, starting with a security needs assessment. Architects can find an excellent resource at www.cpted.net, the website for International Crime Prevention Through Environmental Design (CPTED, pronounced "sep-ted"), an organization based on the premise that the proper design and effective use of the physical environment can lead to a reduction in the incidence of crime.

Atlas sums up the assessment phase of an architectural design as starting with the nature and mission statement of the building - such as hospital/medical, retail, office space, or industrial - and then identifying the potential risks to three primary categories: people, property, and data.

"Take a hospital, for instance," Atlas suggests. "There is going to be a pharmacy, which has drugs that can be targets of theft; there'll be garages and other entry points open during off-hours where people need protection; and there are patient information systems with access points throughout the building and central data storage area, all of which need access and protection."

Atlas uses the CPTED protocol in assessing threats to these areas. From an architectural perspective, much of the solution revolves around vehicular and pedestrian traffic circulation flow within and around the building space. But it also will comprise how security system information can be routed throughout the building. It's a nuanced process, he says. "The attention is often focused on the big events, like terrorism, but in reality you're more likely to encounter a burglary or a disgruntled employee coming in and shooting up the place," he cautions. "The importance is in the details."

Structured cabling is a key issue. Cabling must service a huge array of security systems and checkpoints, from CCTV coverage to hundreds of door position switches (DPS) - electrical contact points that tell a central security position the status of every portal in the structure. In addition to electrical security systems, there are also infrared (IR) and vibration-based sensor systems. "That's an enormous amount of conduit just for that that should be built into the basic architectural design," he says.

While video surveillance and other electronic systems are usually at the top of the security agenda, don't assume that that's all that will be required, says Atlas. "There was an incident in Miami not long

Security Design, Miami, delineates the roles that the three main participants in security systems play:

Role of the client: To define precisely the vulnerabilities and threats to people, information, and property (PIP); to assess the level and cost of protection and the coverage that will be provided; to develop the definition of security needs and provide the architect with a pragmatic description of protection requirements; to define who and what needs protection; to define the assets and the importance of each asset worth protecting.

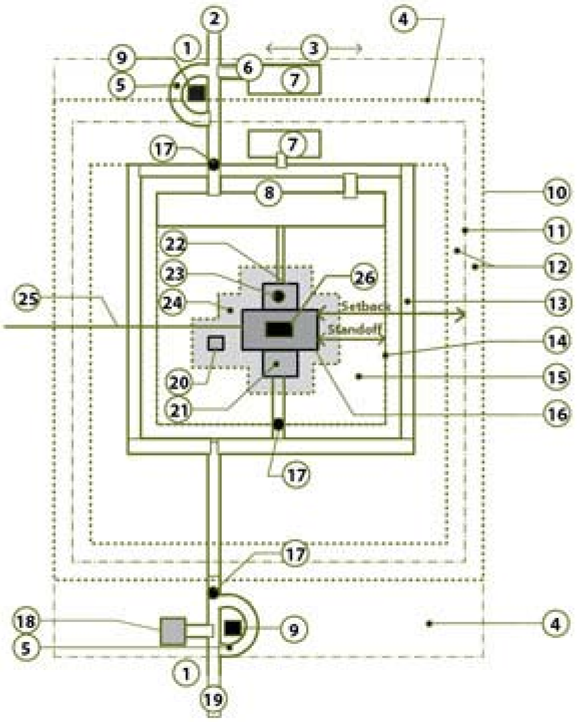
Role of the security manager/consultant: To help the client describe and elaborate the protection requirements and the level of protection required in each area; to help the client assess the threats, security needs, and crime vulnerabilities; to help with the planning of access control, security zoning, target hardening, and surveillance systems; to define the basic security concepts with operational procedures and security manpower allocation; to define the types, location, and tasks of security personnel.

Role of the architect: To incorporate the security program information into effective space and circulation planning; to provide for clear sight lines for surveillance and planned access controls at entrances and exits; to design for the appropriate location of sensitive or restricted areas; to design for the ago where robbers backed a truck up to a Sports Authority store and literally knocked down a concrete wall and loaded goods out through that hole."

That's why those with experience in security matters stress that architects and system designers and installers converge their agendas early in the design stage.

David Stone agrees, pointing out a common mistake at the nexus of architectural and system layout. "The biggest problem is failure to provide adequate space for both equipment and cabling," he explains. "Usually, equipment closets on each floor are on a vertical rise path" - i.e. one atop the other sequentially per floor - "and on a vertical line with electrical [power] cabling. That leads to congestion in the conduit path." Furthermore, the equipment closets that this conduit serves are also getting squeezed. A 2-foot rack now encounters code specifications that call for 3-foot clearances front and back; wall-mounted equipment will add another foot or two, resulting in 10- by 10-foot space needed on each floor.

Planning Concepts For Site Security



1 - Signage
2 - Employee/Visitor Access
3 - Public Image
4 - Uncontrolled Area
5 - Reject Capabilities
6 - Adequate Queuing Length
7 - Visitor Parking (External or Internal)
8 - Staff Parking
9 - Security Post
10 - Site Boundary/Property Line
11 - Perimeter Fence
12 - Clear Zone
13 - Inner Vehicular Circulation
14 - Vehicular Barriers/Inner Perimeter
15 - Vehicle Exclusion Zone
16 - Hardened Building Perimeter
17 - Access Control

planned placement of security personnel; to provide architecture that uses design elements to closely coordinate security technology and personnel. The architect or design professional will need many aspects of information from the owner client and 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.

Feature -Go to other articles like this.
Security - Go to other articles in this category.

18 - External Material Inspection Facility (Optional)
19 - Service / Employee Access
20 - Redundant Emergency Utilities
21 - Loading Dock
22 - Building Lobby
23 - Pedestrian / Visitor Facility Access Control
24 - Clear Zone
25 - Incoming Utilities
26 - Critical Asset

Note: Not all elements are required for all facilities, based on the outcome of a threat and risk assessment.

The problem will only become worse over time, as more and more sophisticated security system components are implemented.1 Allowing for extensive structured wiring in the design stage is important, but ultimately, depending upon the level of security a building requires, it may just be delaying an inevitable move to alternate signal transmission methods. "There's only so much conduit that you can run in a poured slab before you begin to undermine its structural integrity, as well as interfering with the efficiency of the conduit itself," says Stone.

One solution is to switch cable type. Fiber-optic offers considerable capacity in far less space than coaxial cable. Although only certain types of equipment can utilize fiber-optic wiring, it will still reduce conduit capacity or, more importantly, allow what conduit there is to have some room to add more cabling in the future. Some data streams are wedded to copper, such as telecom providers, so any reduction in cable size, when it makes sense, is welcome.

Wireless is another solution. More and more building security systems are using a node-and-repeater or Wi-Fi approach buildingwide. Here, too, though, the architect must accommodate that in the structural design. Line-of-sight is optimal for wireless systems; that could affect placement of both load-bearing and aesthetic walls, as well as wall composition. Lead, commonly used in medical applications near X-ray or radiation-based treatment areas, stops wireless dead in its tracks. At best, a building will have to contend with a hybrid of wired and wireless data routing for its security systems.

Creating Secure, Viable Spaces

New York-based architect John Storyk specializes in media facilities that must constantly move data around securely. He says architects should be concerned about conduit, access points, and creating a viable central space within a building that data hub devices and humans can comfortably share. "Humans are your front line of security, so don't shortchange them in the design of your central machine room," he says.

A central data operations center will handle the movement of both security and other information. For instance, in a hospital, patient information and security camera signals will route through centralized servers, assuring both types of information the same degree of security. This also helps in planning wiring runs.

(Increasingly, residential designs are using the building's main 110-volt power runs to carry low-bandwidth data such as audio. While that concept could be applied to commercial structures, many architects resist the idea. "The AC lines are simply not robust enough at this point," says Storyk. "Maybe someday in the future - people are working on it - but not today.")

Protecting the Front Lines

Members of ASIS International, an Alexandria, VA-based trade group for security professionals, increasingly interact with architects, says Rich Grassie, chairman of the organization's security, architecture, and engineering council. "There may not be any single-source security solutions that architects can wrap their design around, but there are numerous security technologies that have significant impact on the design of the space and the structure," he says.

Lobbies are the front line for this intersection: Access control systems such as optical and mechanical turnstiles require that architects understand the flow rate that such systems are capable of in order to design in sufficient holding-area space on either side of the barriers. "That ties in further with knowing the speed, capacities, and cycle rates of the elevator banks of a building," says Grassie. "The whole point is to keep the flow moving smoothly, and that's a function of design and technology."

Grassie also recommends that architects be aware of the properties of the current generation of laminated glass and glass-film products designed to increase overpressure resistance (from blasts and hurricane winds). "They can also help protect against vandalism," he says, no small consideration for companies such as biotechs that use animals for research purposes or any company whose work may cause it to become the target of sometimes violent activists.

Technology will keep changing, but the purpose of security will not. Architects are well-advised to stay up on how the technology of building security continues to evolve so they will be able to long admire their own work.

1Footnote: It's worth noting that there are no true single-source security solutions for commercial or industrial buildings; solutions are still component-based, necessitating a security systems consultant to coordinate them. Residential construction, however, has an increasing array of single-source security solutions to choose from. It's possible that some of those integrated products may migrate to commercial construction in the future.

Links referenced within this article

Click Here for Related Products
http://www.architechmag.com/spotlight/2006/Tracking.asp
Feature
http://www.architechmag.com/articles/Storytype.asp?ArticleID=3114&StoryType=Feature
Security
http://www.architechmag.com/articles/related.asp?ArticleID=3114&Category=Security
"Terms of Use"
http://www.buildings.com/Misc/termsofus.asp
www.marketingreprints.com
http://www.marketingreprints.com