Designing Security Measures

Timothy (Tim) Corbett

Following the attacks of September 11, 2001, security features in buildings and sites have become extremely important. Architects and Engineers (A/E) help diminish the potential risks inherent in a building, site, and facility by developing design solutions that address security measures and integrate security into the overall building and site design. This concept extends far beyond the protection of doors and windows.

Designing and integrating security into buildings, structures, and landscapes can assist greatly in diminishing potential risks. Crime prevention and security officers throughout the country today are working with A/E firms for the sole purpose of improving security measures within public and business communities. In the past, traditional security designs had incorporated blocked access strategies using reinforced concrete walls, bunkers, or fortress design concepts, locking mechanisms, alarms, and other security features. In many cases, retrofitting security measures to current structures and sites was incorporated following the 9/11 attacks. These measures may be effective, however incorporating unattractive and un-aesthetically pleasing security measures affecting flow of personnel and traffic that negatively impacts a company image, not to mention the physiological effects on employees and customers entering these sites.

With appropriate site assessment and architectural design features, effective security components can be incorporated into the design that are both aesthetically attractive and pleasing. For security measures to be effective as well as attractive, design professionals should refrain from the "bunker" design concepts mentality. Effective security concepts can be accomplished by initially evaluating the potential risk and – with the collaborative efforts of security professionals, A/E firms, owners and developers – can develop solutions that address security measures integrating security into the overall building design. This approach will assist in diminishing potential risks inherent in a building, facility or site. Design solutions should balance the security requirements, openness of the site, and the overall building cost.

Security Assessment

The first step in identifying design security measures is performing a Security Assessment of the building, site, or facility. A Security Assessment identifies vulnerabilities as; physical or operational weaknesses in building facilities that could be exploited. The main purpose of vulnerability analysis is to identify the exposure of assets to potential risk and threats. Asset vulnerability information is used to determine the protective measures of current buildings and to assess the extent to which additional protective measures may be necessary for further protection. Security options shall be based on the security assessment and associated cost for security measures.

The building security assessment is a specific activity performed during a project's design phase. Security assessments are performed for both new buildings as well as renovation projects. Security assessments can vary greatly, but the main considerations are the building occupants and the organizational assets. At risk are the people and the physical infrastructure including the building structures, systems, electronics including the computer and communication systems, and propriety information.

The first step is defining the scope of the security assessment. That is based on the owner or corporation's need combined with their ability to respond to security incidents. The incidents can range from basic security concerns to direct attacks on corporate assets. The following tasks should be considered in security assessments.

- Building security control and hours of operation
- Personnel screening policies and procedures
- Personnel security policies
- Site and building access control
- Video surveillance, assessment, and storage
- Natural surveillance
- Internal and external security incidents
- Integration of building security systems
- Shipping and receiving security
- Property identification and tracking
- Proprietary information security
- Computer network security
- Workplace violence prevention
- Mail screening operations and procedures
- Parking garage security
- Communications security
- Executive protection
- Business continuity planning and evacuation procedures

Each project design team consists of an architect, structural, mechanical, electrical engineering personnel, landscape design and others depending on the project. Each team member integrates security concepts, strategies, and measures into their design process. The security assessment process culminates in the determination of functional design requirements and recommendation of strategies for achieving the desired levels of protection, from which the client can select the strategies it deems most appropriate based on their operations, budget, and other considerations.

Cost-Benefit Analysis

With every project, there are security design options. The question is, "Which options and at what cost?" Included in the security assessment should be considerations of the cost versus the potential benefit of a security measure. A security professional can assist design professionals in determining actual costs of implementing design security features against the potential impact of a loss. For example, it would make no sense to spend $50,000 on a security measure to prevent the theft of a $1,000 item, especially when it may make more sense to purchase insurance or remove the item to a more secure location. Forecasting individual loss events and their probability or frequency will also assist in identifying security options and related costs. Identifying loss events or associated risks, conditions, circumstances, objects, activities, and relationships for producing them should be part of the cost benefits analysis.

Cost-analysis is important when considering security measures, however, the decision as to what measures should be implemented should not be determined based on only the cost. As stated previously, the most effective method in making cost benefit analysis decisions is weighing the risk factors, considering the maximum loss due to substantial interruption of corporate or individual activity, direct cost loss, indirect cost loss, replacement cost loss, and future cost loss due to events, whether implicated

directly or not. Often owners or corporations will spend a dollar to save a dime. It is always more important to properly prepare for a disaster and not need that preparation than to need it and not be prepared.

Building Owners' Perspective On Security

Building owners and corporations are focused on their biggest asset, their employees and the protection of their property. As an owner becomes more in-tune and educated about potential security concerns, they begin to focus on the continuity of their business. That would include intellectual capital, data preservation, the corporate image that could be affected by security breaches including financial fall-out of company stock prices and consumer confidence. Owners should focus on security measures and solutions with an open and effective design, implemented with reasonable costs and minimal interference with business operations.

Because of a sudden natural disaster or terrorist attack causing building damage, utility service interruption and loss of access can be debilitating for any company. The longer a company does not operate, the greater risk that company has of not resuming operations. Immediate loss of revenue is the main concern along with the affect on a company's bottom line. It is important to identify security measures and strategies needed to respond to each type of disaster event.

Owners are concerned with critical information and data that must be protected against possible security breaches. This information is needed to sustain business operations or restore operations following a disaster. This may be addressed through a data redundancy program, merging security and information technology departments. Understanding which functions will resume operations is the first step of preparing a disaster recovery plan.

Design professionals must design security measures in an effective manner. If they are ineffective, people will resist them and eventually find ways to bypass them. Security elements are customized for specific buildings and structures creating a safe work environment. Security measure will vary from region, city, state, building type, and business enterprise – there is no one single solution. However, when architects and engineers evaluate the owner's needs, understanding the business operations, along with obtaining input from security professionals, proper security measures can be identified and incorporated.

Designing Security Zones

When designing security solutions, it is helpful to design in a series of zones with varying security requirements. Using an onion as an example; the outer layer is the protective shell for entry, then one must go through various layers as one moves inwards. A similar concept is used when designing security measures – focusing on securing the critical assets in central locations is much more effective, and less costly, than trying to protect assets in multiple locations.

Crime prevention through environmental design (CPTED) provides guidance in designing crime prevention strategies. CPTED strategies may be used in a number of combinations and provide for a clear border of definition of controlled space. Boundaries may be identified physically or symbolically. Fences, shrubbery, or signs are acceptable border definitions.

The following are considerations when designing security zones.

- **Transitional zones**: It is important to clearly mark transitional zones on moving from public, to semipublic, to private.
- **Gathering areas**: Formally designate gathering or congregating areas in locations with good natural surveillance and access control.
- **Safe activities in unsafe locations:** This strategy is used on school campuses, parks, offices, or institutional settings. Safe activities serve as magnets for normal users who exhibit controlling behavior, and tell abnormal users they are at greater risk of scrutiny or intervention.
- **Unsafe activities in safe locations**: Placing vulnerable activities near windows of an occupied space within tightly controlled areas helps overcome risk.
- **Natural barriers**: Activities can be separated by distance, natural terrain, or other functions to avoid fear-producing conflict.
- **Scheduling of space:** Generally, it has been found that the effective and productive use of spaces reduces risk. Abnormal users feel at greater risk of surveillance and intervention of their activities in well-organized spaces.
- **Natural surveillance**: The perception of surveillance is a very powerful security tool. Windows, clear lines of sight, and other natural techniques are often an effective use of mechanical or organizational methods.
- **Distance and isolation**: This is accomplished with improved communication and design efficiencies of natural surveillance.

Building Hardening & Security Products

In densely populated structures and urban areas, blast standoff distances are not available. In these situations, the design option for hardening the building structure is used. Hardening is accomplished through the selection of products and materials that increase the structural integrity of the building's mass, creating a stronger foundation and exterior layer, and decreasing the number of openings in the exterior layer, such as windows. When selecting windows, a blast curtain concept is considered, absorbing the force of the blast rather than resisting as a building exterior wall would. The purpose of blast curtain windows is diffusing a bomb blast that traps glass before entering the interior of the building and causing injury to building occupants.

For buildings that require a high level of security based on the defined scope by the owner, materials and products that contribute to security features such as glass, cladding, monitoring equipment, and bollards must be considered in the early stages of design. This early identification assists in the integration of such materials and products. The American Society for Testing and Materials (ASTM) has identified security-related standards, however, has few recognized definitions for "secure" building products. There has been little industry consensus on terminology related to security design, and few recognized methods for the testing of products' performance. Architects and engineers must perform their own due diligence in specifying security-related products with specifications for security materials based primarily on function and performance. To assist this effort, the architect or engineer should determine if the product is appropriate for the level of protection desired. For example, "Does it provide adequate protection or does it provide excessive protection for the building?" Cost should not be the primary determining factor, however it plays a part in the decision-making process when selecting a product. Products and equipment designed to enhance security are often specialized and expensive and may affect the cost of other building systems. Bullet-resistant glass is substantially thicker and heavier, and costs significantly more than conventional glass. The structural components of the building would require enhancements for the additional weight of the glass and load-bearing capacity thereby adding to building expenses. Security products and special order products also may have a long lead-time from manufacture and delivery.

Research into the availability of the products and ordering at the earliest opportunity is important. It is also important to check security related products for compatibility with local building codes.

Parking Structures

The security objective of a parking facility is to provide safe and secure vehicular parking environments in configurations that may include surface parking adjacent to a building, surface parking remote from a building, a stand-alone parking structure, or an interior parking area in a building containing other uses. A parking structure is one of the greatest areas of concern for security professionals so great care and consideration should be used in their design. Based on open access for most vehicles, including trucks, parking structures are one of the most vulnerable areas for a building.

There are several design options to consider. Depending on a parking facility's location and proximity to critical buildings, hardening of the parking structure may be an option. Parking areas within buildings have the greatest threat and access should be designed through controlled entry points. Whenever possible, interior parking should be designed away from critical business operations. If the building superstructure is supported by the parking structure, blast mitigation measures should be considered. Adjacent and remote surface parking can be designed maintaining lines of sight from the main building by controlling landscaping features no higher than three feet. Remote parking situated with a sufficient standoff distance will mitigate explosive effects on critical buildings.

Mechanically operated barriers and other measures can provide positive control by way of road blockers and rising barrier configuration placed in entry and exit lanes. Exit lanes can have designed barriers that include lifting gates and tire shredders preventing unauthorized entry. Card-based access control systems are used at all doors inside the parking facility with direct access to secured building areas or elevator lobbies. Elevator lobbies servicing parking areas provide free access at all points only when they are separated from main building elevators. Depending on the facility configuration, a mix of pan-tilt and fixed cameras or all fixed or all pan-tilt cameras can be used for surveillance of parking areas. The level of surveillance depends on client preferences, risk assessment, and cost. Security devices inside the parking facility (e.g., intercoms, emergency telephones, area detection and audio detection devices, and automatic video scene call-up for operator assessment) are effective and desirable options. Intercoms are effective for access and egress control gates and elevator communications. Intercoms used in combination with closed circuit television (CCTV) assessment provides an effective security measure.

For any security measure to be effective, parking restrictions should be strictly enforced and operational procedures in place. When it comes to security, there is no substitute for a patrol officer. Security patrols of parking areas should be frequent to ensure safety with contract parking operations personnel having limited security functions and responsibility.

Access Control

Designing methods to control access to the building is a critical security measure. Access control manages individuals entering a building using key-cards, access codes, or other identification methods. Access controls provide additional control and limitations to access into stricter controlled areas within a building structure. Effective access controls require the integration of various security functions that serve as individual layers of protection.

The integrated system consists of the following common access control elements:

- Guards
- Locks – combination, code, or key
- Card reader systems – magnetic stripe, optical barcode, proximity cards, biometric systems (i.e., finger-prints, signature, face or hand geometry, voice recognition, and retina recognition)

Access control vulnerabilities should be identified for the proper security solutions to be identified and implemented. An access control profile must be completed addressing who has access to the building or facility, and when. The access profile will assist in identifying the security processes and tools needed to appropriately design and implement effective access controls.

Access Control Systems (ACS) integrates hardware and software allowing monitoring of control access and recording facility access attendance. Access Control Systems can be used in the following scenarios (Lexington Technology Security Systems, 2007):

- Stand-alone system: A stand-alone system provides benefits of a low cost, easy to install, and convenient for special security requirements and small offices. It typically requires installing hardware, only, without any host computer. The down side of choosing a stand-alone system is the limitation of a small-scale installation, and the increased difficulty to change access permission.

- Network ACS: A network ACS offers a wide range of options. Systems are capable of supporting simple access to advanced requirements needed to integrate access control, alarm monitoring, fire protection, CCTV, security badge and more in one centralized system.

For larger security systems (those supporting hundreds of readers, alarm points and multiple workstations), multiple operators can simultaneously monitor a facility at real time. Such systems support third party equipment like CCTV and video recording devices. Systems can support major identification technologies like proximity, fingerprint, iris scan, facial recognition, hand geometry, mag, Wiegand , infrared, barcode, etc. Controller use high-speed communication equipment serves to ensure efficiency and reliability. Totally integrated employee time and attendance tracking solutions are also available with these types of ACS.

Site Planning & Design

Landscape architects are playing a key role in developing security measures through site planning strategies incorporating landscape protection elements. Identifying security measures with the integration of aesthetic quality is a goal of landscape architecture. Following the attacks of 9/11, many cities, company buildings, and perceived-as-vulnerable sites were protected by concrete barriers and pre-cast concrete planters, to limit access. These barriers were placed initially as temporary fixes, however as time went on these barriers became more permanent at certain locations. Many barriers were placed as a knee-jerk reaction without considering the true vulnerabilities through a risk analysis. In addition, most barriers were dropped into place without proper anchoring, providing only limited protection.

Numerous guidelines have been developed to assist designers and owners in making decisions regarding security for site planning and landscape design techniques. Design periodicals have focused on public spaces such as the National Mall in Washington, D.C., federal buildings, and urban streetscapes. Also,

anti-terrorism design standards developed for new military projects have been and are being mandated. Private owners are dealing with the same issues with private corporations installing physical pre-cast concrete barriers without first completing a risk assessment that properly identifies vulnerabilities. Companies, schools, and government facilities are reevaluating options by using a security analysis to identify proper security site planning and landscape measures. The following provides information identifying security considerations to be evaluated for enhancing site safety and security.

- Location: Security measures in urban settings vary from suburban settings. Urban sites usually have limited space for perimeter security with structures outlined by sidewalks or streets. Security measures should involve "hardening" street elements to establish a barrier such as the use of raised planters and bollards establishing setbacks for vehicle zones. Suburban sites usually have more land to incorporate security measures such as landscape berms, changing terrain levels, natural barriers, incorporating perimeter fences, and guard stations separating structures from parking vehicle zones. Proximity to fire and police stations, hospitals, shelters, and other critical facilities that could be of use in an attack should also be a consideration.
- Adjacent Structures: Consideration should also be given to facilities, structures, and operations with adjacent businesses and facilities. One business may not be a terrorist target, however, an adjacent site may be. Security measures for a site that may not be a primary target, but adjacent to one that is, should be considered.
- Code Compliance: In most cases physical improvements to any property requires a review and approval by local zoning authorities. Design security measures and upgrades must comply as well and should consider building codes, review, and approval processes required in that area.
- Vehicle Access: Using vehicles for terrorist attacks remains a high-risk for sites. Controlling vehicle flow and access is critical for the security and safety of a site. Careful consideration and planning is required in the configuration of vehicular access maximizing security, however, also considering traffic flow, volume and visual aesthetics of the site should be included. The various types of vehicles must also be considered such as those of regular employees, visitors, deliveries and service providers. Separating traffic types is vitally important for the safety of the site. Service entrances and loading docks should be located away from areas with concentrations of employees and visitors, particularly main entrances and gathering locations such as plazas. Road alignment is important including drop-off points, and the proximity of parking to building structures. Curved designed driveways or roads that do not directly align with a building's entrance reduces vehicle velocities towards a building, thereby reducing the option for a vehicle being used as a battering ram into a building.
- Public & Gathering Spaces: The design distances between buildings and gathering places, parking areas, and plazas should be maximized whenever possible. Spaces allowing public access increase risk. Increasing distance between these locations and the main building decreases potential blast effects on the structure. Gathering spaces should also have open visibility for security observation.
- Natural Security Barriers: Using naturally areas and large trees are excellent vehicle barriers. During site planning and design, saving as many trees on the site away from the building provides security enhancements. However, ensure visual security observation is not obstructed by the location of the trees. Site waterways, streams, drainage ways, and ponds are also excellent natural security barriers.

Comprehensive site planning that encourages certain types of development, incentives, allocation of resources, and capital improvement programs improves security measures of sites and maximizes protection measures. During the design phase, external and internal land use design concerns, including the characteristics of the surrounding area such as construction type, occupancies, and the nature and

intensity of adjacent activities as well as the implications of these characteristics for the protection of the employees, should be prime considerations. The amount of land available on the site for standoff and the inherent ability of the site to accommodate the implementation of natural and man made antiterrorism and security design features assist designers selection of security measures.

Building functions and building layouts, depending on site characteristics, the occupancy requirements, and other factors, may allow for clustering key functions in one particular area, or may have these functions designed in a more dispersed manner. Both patterns have compelling strengths and weaknesses in terms of security. Concentrating key functions in one place may create a target-rich environment and increase the risk of collateral impacts. Additionally, it increases the potential for the establishment of more single-point vulnerabilities – such as indicated if these areas become a target, the company or site may be closed for a substantial period of time if an attack occurs at one of these locations. However, grouping high-risk activities, concentrations of personnel, and critical functions into a cluster can help maximize standoff from the perimeter and create a "defensible space." This also helps to reduce the number of access and surveillance points, and minimize the size of the perimeter needed to protect the building areas. In contrast, the dispersal of key functions reduces the risk that an attack on any one part of the site will impact the other parts. However, this approach has an isolating effect, reducing the effectiveness of on-site surveillance, increasing the complexity of security systems and emergency response, and creating a less defensible space. When focusing on a specific site, the economics and other critical factors as referenced above should be thoroughly considered when designing site planning and security measures.

Conclusion

Following the attacks of 9/11, security features in buildings and site planning has become extremely important. This paper identified key security design solutions that should be considered including; performing a security assessment, cost-benefit analysis, owners' perspectives of security, building hardening, access control, parking structures, and site planning. These topics are vitally important when designing and integrating security measures into buildings, structures, and site planning. If these topics are properly addressed, potential risks can be greatly diminished.

When vital information is obtained through evaluating real and potential risks and vulnerabilities, appropriate security measures can be developed through the collaborative efforts of security professionals, owners, developers, architects, engineers, landscape professionals and related firms. When done and managed correctly, and with knowledge of the industry's needs and concerns, designing and implementing security solutions can be effectively integrated to balance security requirements, openness, appearance and overall cost of these projects.

_____

Timothy (Tim) Corbett is Founder and President of SmartRisk, a Pasadena, CA based consultancy providing risk management solutions to Design and Building Professionals. Mr. Corbett holds a BS Degree in Security & Risk Management, Bellevue University, MS Degree in Management Regis University, Denver, a degree in Environmental studies as well as concentrated studies in Architecture Design. As a recognized expert, Tim is a requested speaker at regional and national forums and published on the topics of insurance and risk management. For more information on this or other topics, Tim can be reached @ P: 626-665-8150, E: tcorbett@smartrisk.biz or visit SmartRisk's website at www.smartrisk.biz.

_____

This article is intended for general discussion of the subject, and should not be mistaken for legal advice. Readers are cautioned to consult appropriate advisors for advice applicable to their individual circumstances.