

Security Evaluation and Planning

Marco A. Monsalve and James R. Sutton

Security evaluation and planning services help building owners determine the levels of security protection for their building facilities and provide architects with security design criteria to use in building design.

The expanding need for security assessment of building facilities stems from growth in terrorism, transnational crime, business fraud, environmental concerns, and political activism. To help clients address threats posed by these activities, architects can avail themselves of specialized knowledge and skills aimed toward making buildings more secure.

Law enforcement and intelligence authorities around the world acknowledge that attacks against buildings, including use of nuclear, chemical, or biological agents, is not only probable but inevitable. Even setting aside such incidents, the facts—clearly documented in the daily news—demonstrate that such acts are increasing in frequency worldwide with no signs of abating in the near future. Adding to such threats are the efforts of single-issue political extremists, anarchists, and similar autonomous actors engaged in sabotaging commercial, government, and public facilities.

CLIENT NEEDS

Historically, the ability of buildings to protect people from natural and man-made threats largely depended on the technology available, the requirements of clients, and the risks inherent in the environment. While this is still the case for buildings in both public and private sectors, it is important to remember that most firms and organizations find it difficult to quantify security as an expense that has a return on investment. Consequently, in the private sector security is often undertaken with limited resources.

Not all buildings are the same, nor do they face equivalent threats. Facilities most likely to suffer attacks and those most likely to warrant security assessment are not necessarily the

MARCO A. MONSALVE is president and CEO of McManis & Monsalve Associates, a management consulting firm in Centreville, Virginia, that specializes in developing strategic and operational security plans for major government facilities. James R. Sutton has extensive experience in threat assessment and critical incident management. A former FBI agent and director of asset protection for Sears, Roebuck, he is currently an intelligence analyst with a government agency.

Summary

Why a Client May Need These Services

- To protect human and physical assets
- To ensure operational continuity
- To minimize legal liability
- To reduce insurance costs

Knowledge and Skills Required

- In-depth knowledge of security operations
- Ability to conduct threat and vulnerability assessments
- Ability to conduct risk assessments
- Knowledge of current surveillance technology
- Understanding of legal dimensions of security programs
- Strong communication skills

Representative Process Tasks

- Asset analysis
- Threat analysis
- Vulnerability analysis
- Risk analysis
- Identification of security measures

► **Ranked from highest to lowest level of incidence, the following facilities experience the highest incidence of security events and attacks:**

- **Businesses**
- **Industrial facilities**
- **Government buildings**
- **Public transportation hubs**
- **Entertainment venues**
- **Schools**
- **Residential buildings**

► **Facilities requiring the highest level of protection from security events and attacks include the following:**

- **Government facilities**
- **National infrastructure elements**
- **Public service facilities**
- **Facilities in high-risk areas**
- **Controversial or targeted activities**

same. A study by the authors disclosed that the highest number of security-related incidents, ranging from workplace violence to attacks by militant activists or organized crime, occurred in businesses and industrial facilities. Government buildings with significant unrestricted access to the general public were the next most common site of incidents. In addition, incidents occurred more frequently in locales where large numbers of people congregate, although with rare exceptions, most of these were high-probability, low-consequence events.

Facilities such as those involving key government operations (economic, military, executive, national security) are more likely to suffer low-probability, high-consequence attacks. Such attacks are normally carried out by committed, trained paramilitary cadres equipped with appropriate technology and operations intelligence. These individuals have made a rational cost-benefit analysis of their actions and are willing to assume the risk and consequences of carrying them out.

Client Security Objectives

The security objectives of the client may be varied and complex. However, the objectives will generally fall into three major groups: protecting assets, maintaining continuity of operations, and minimizing insurance costs.

Protecting Assets

The desire to protect assets—including people, property, and information—beyond the level of protection afforded by building codes is driven by several factors. Moral and ethical imperatives form the basis for protecting people who occupy and use buildings. Coupled with this, maintaining financial integrity and profitability affects the desire of building owners to minimize or prevent damage to or loss of their buildings and the contents in them. More subjective psychological factors may shape desires to keep up physical appearances that can affect how organizations and businesses are perceived.

Maintaining Continuity of Operations

For some clients, operational continuity may be the most important objective. Experience in the last 50 years shows that the failure of critical infrastructure components (water supply, electric power, telecommunications, health and safety systems) can cause significant economic losses to an enterprise and can have a profound impact on an organization's technical, administrative, social, and economic standing. The demand for safety and reliability in buildings and building systems has increased at the same time performance standards are escalating. Not surprisingly, infrastructure failures tend to attract negative publicity out of proportion to the outcome. As a consequence, the issue of business continuity, often predicated on having a degree of redundancy designed into critical systems, will become an increasingly important element in corporate and business planning. This will sometimes call for protection responses that exceed what codes normally require.

Minimizing Insurance Costs

In the past, building owners rarely accepted the need for security measures against terrorist threats, since these types of attacks were infrequent and insurers were less likely to offer credits for well-protected facilities. Historically, most insurance policies covered the cost of repairing or replacing buildings due to the effects of terrorist attacks. Although financial backers of major projects require significant insurance to cover replacement of a structure, most do not require coverage for collateral losses that could potentially affect tenants, such as loss of market share, damage to corporate or product image, or productivity losses during recovery. Such losses normally account for the largest economic impact on an affected property. Tenants located in a facility incorporating increased security protection may be able to negotiate more favorable insurance rates to cover their losses.

Security Perspectives of Stakeholders

Assessing the safety and security requirements of clients ultimately depends on effectively balancing the perceptions of project stakeholders who may have divergent security goals. Practical and cost-effective security planning will creatively consider and balance these differences.

World Trends and Security

The National Intelligence Council (NIC), serving the director of the CIA, provides long-term strategic analysis by drawing on nongovernmental experts in academia and the private sector for fresh perspectives to enhance U.S. intelligence posture. The NIC report *Global Trends 2015: A Dialogue About the Future with Non-Government Experts*, issued in 2001, identified major trends and drivers shaping the world in the decades ahead. The study highlighted the following drivers:

- *Demographic.* Barring a major worldwide catastrophe, world population will increase from 6.1 billion to 7.2 billion by 2015. This growth, in combination with other demographic factors, will place a significant strain on the social contract, will leave significant shortfalls in the size and capacity of the workforce, and will inexorably lead to social conflict.
- *Natural resources.* Overall food production will be adequate to feed the world's growing population, but poor infrastructure and distribution will precipitate pockets of chronic poverty and social instability.
- *National and international governance.* Technology and globalization will increase the transparency of government decision making, complicating the ability of authoritarian regimes to maintain control, but also complicating the traditional deliberative process of democracies. Even in developed countries, the political process is likely to become increasingly confrontational and acrimonious.
- *Conflict and criminality.* Asymmetric warfare will increase conflicts between conventional military forces and irregular militias, including heavily armed criminal organizations. In this context, developed countries are facing an upsurge in low-intensity conflicts that include actors capable of using crude but effective weapons. Protagonists consist of an ever-increasing number of political, ethnic, and religious extremist groups. Increased globalization—driven by information technology—will allow increased interaction between criminals and extremists and will provide them with greater access to financial sources, increased access to employ sophisticated deception and denial techniques, and greater ability to communicate with each other.
- *Natural disasters.* Demographic pressures and technological developments have resulted in the development of areas historically prone to natural disasters such as floods, droughts, and earthquakes. While the impact, location, and timing of such events are not predictable, they are likely to lead to major changes in migration patterns, the economy, and social stability, with worldwide repercussions.

Owners

As the primary project stakeholder, the owner's opinions, needs, and perceptions about security will carry the most weight. However, the owner's perception of risk and the need for security—while worthy of consideration—may not be rigorously objective. There may even be cases in which an owner's perception of risk does not coincide with the assessment conducted by financial backers of the project.

Financing Entities

The security opinions of financial backers of a project who shoulder considerable economic burden and risk are often as important as the owner's. This is particularly true because financial entities represent established institutions with significant experience in risk management and threat assessment. Rather than mandating specific security solutions, financial backers are likely to articulate security objectives and ask the project team to explain how its design meets them.

Regulatory Entities

Authorities having jurisdiction (AHJs) are the federal, state, and local agencies responsible for ensuring that the health, safety, and welfare of building users and occupants are addressed. AHJ staff members employ requirements and standards mandated in codes and other regulations to review building design and construction. However, building codes generally do not address security issues. Thus, a building that meets code and is

otherwise safe may not meet expected security needs. In this case, the architect and project team will be challenged to achieve a balance between mandated safety criteria and criteria required to achieve the desired level of security protection.

SKILLS

There are few, if any, easy answers to incorporating security concerns into building projects. Risks are not always quantifiable, and when they are, statistics can be deceiving and offer little help in predicting low-probability, high-consequence events. Overcoming actual or potential security challenges requires sophisticated analysis and sensitivity to nuances. Frequently, solutions involve technical considerations or consequences that are best understood by experts in the field.

Obtaining an understanding of fundamental security concepts, however, can help architects qualify and engage security consultants, cogently discuss security matters with project team members during predesign activities, and achieve responsive security solutions in the design phase. Several of these security concepts are touched on below. The “For More Information” section at the close of this topic lists references that address these subjects in greater depth.

Crime Prevention Through Environmental Design

CPTED is a comprehensive planning process appropriate for addressing both criminal and terrorist actions in the built environment. Although these actions may have different motivations, they have certain commonalities that make the application of CPTED appropriate as a singular strategic approach. CPTED emphasizes a fact-based evaluation of foreseeable problems and development of security measures to deal with them. The process is initiated with a threat identification and vulnerability analysis that documents actual or potential exposures and acknowledges that effective building design can minimize opportunity for criminal activity.

This multidisciplinary CPTED process relies on access control, natural surveillance, territoriality, management, and maintenance to support legitimate activity in the built environment and is predicated on the effective use of internal resources to reach its goal. The process applies various concepts that fall within the following categories:

- Natural strategies (site design, spatial planning, architectural design)
- Mechanical strategies (technology and hardware)
- Organizational strategies (people, staff, procedures)

The objective of CPTED is to reduce opportunities for crime and other illegitimate behavior in and around buildings. Primary CPTED goals include increasing the probability that suspicious activity will be observed, interdicted, and neutralized; increasing the effort required to commit an act of crime, workplace violence, or terrorism; and removing the excuses for noncompliant behavior. Means for achieving these goals include surveillance and supervision of the space, creation of real and symbolic barriers that make access to targets more difficult, and clear signage, statement of rules, and border definition.

Security Layering Concept

The concept of security layering can be visualized as a series of concentric rings, with the outermost one being the site perimeter. Moving inward, the building envelope represents another ring or line of protection. Additional layers are further defined by zones within the interior that progressively work toward the center of the building. This layering concept is useful for thinking about how to enhance defensive components during the building planning and design process. For example, highly sensitive and critical areas can be located closest to the center of the building, where they can be afforded further protection with security equipment and devices. Main entry points in the envelope can be controlled with graduated levels of access and built-in monitoring systems. The outer envelope can be designed to be more resistant to the effects of hostile actions. The out-

ermost perimeter (usually the property line) can incorporate various barriers and means for controlling vehicular and pedestrian access to the property.

Building Hardening Techniques

Building hardening may embody several objectives, including improving the ability of a building to withstand the effects of bombing and ballistic attacks and delaying the time required to gain access by forced entry.

Mitigating Blast Effects

Blast mitigation is intended to minimize loss of life and property by avoiding or delaying structural failure (progressive collapse) so that occupants can be safely evacuated. Structural and nonstructural considerations are needed to address the blast effects of conventional explosive devices.

- *Shock waves.* These are compression waves sufficient to damage glass and building exterior wall components. They can destroy structures at close range.
- *Blast overpressure.* Typically this consists of very-high-amplitude loading of very short duration and only one cycle.
- *Fragmentation.* Most explosions produce high-velocity fragments of glass, masonry, and vehicle parts. These fragments often cause most of the casualties in an affected area.

Blast-resistant structural analysis requires skill in specialized computer modeling coupled with experienced engineering judgment. In the design phase, the results of this type of analysis are combined with engineering of structural systems and components. Nonstructural strategies to mitigate the effects of explosions include maximizing the stand-off distance between possible detonation points and the building, securing the site perimeter, using building shapes that better resist blast shock waves, and applying CPTED strategies such as controlling approach patterns to the building and eliminating or strictly controlling parking beneath facilities.

Mitigating Ballistic Attacks

Depending on the anticipated method of ballistic attack, architects can plan for and incorporate a variety of design elements that include fortified walls, armor, and window film to minimize splintering. Ballistic assaults may involve weapons such as high-powered rifles, rocket-propelled grenades, light antitank weapons (as was the case in the Puerto Rico office of the FBI in 1983), mortars, and even guided missiles.

Mitigating Forced Entry

To better resist forced entry into buildings, the American Society for Testing and Materials (ASTM) has developed a number of tests and performance specifications for doors, windows, curtain walls, and impact protection systems. Along with using more resistive building components, some corporate facilities, embassies, and government buildings are including “safe rooms” designed to protect senior executives in the event of attacks. Some rooms are equipped only with panic alarms and metal doors. Others are designed to resist armed attacks and breaching efforts by means of explosive charges.

Chemical, Biological, and Radiological Protection Techniques

Public safety authorities in the United States are preparing for deliberate or accidental releases of chemical, biological, and radiological (CBR) agents. Strategies and techniques for protecting building occupants from the effects of these substances largely depend on whether the release occurs inside or outside the building, and should consider both immediate and long-term actions to safeguard buildings. Technologies to address CBR threats are in a constant state of flux, and considerable effort and time are needed to keep abreast of these developments. Most professional security consultants, particularly those specializing in counterterrorism, conduct significant research on these issues and are likely to be familiar with the latest developments.

Government Security Guidelines

Standards in the federal government require security assessments to provide a defined level of protection (LOP) with specified countermeasures. When the LOP is defined, the countermeasures are priced and the contract officer has the option of selecting appropriate measures depending on a prudent level of protection and the cost-effectiveness of the measures.

Security standards developed by the Government Services Administration (GSA) encourage defensible space and crime prevention through environmental design (CPTED) approach to clearly define and screen the flow of persons and vehicles from public to private spaces.

GSA has developed a set of criteria with four levels of protection for every aspect of security. These standards address the functional requirement and desired application of security glazing, bomb-resistant design and construction, landscaping and planting designs, site lighting, natural and mechanical surveillance opportunities, window placement, proper application of surveillance equipment, and so on.

Security Consultants

Many contradictions and ironies exist in security planning. There are rigid rules, but there are also many exceptions. Architects may want to call on experts in the security field for consultation and advice.

The most important attribute a security consultant can offer is objectivity. Consultants must be able to exercise discretion and professional judgment rather than acquiesce to transient pressures or demands. In addition, those not aligned with specific products, manufacturers, or service providers (e.g., guard companies) are often better able to provide objective consulting services.

Security experts sometimes develop additional specialization within their disciplines, such as counterintelligence, antiterrorism, special operations, asset protection, covert entry forensics, data encryption, access verification and control, security management, critical incident handling, or development of training/continuing education programs. The skills and in-depth understanding of these security experts equip them to help architecture firms mitigate risks from these threats in their building designs.

Contractual and Legal Considerations

There is no change in the legal standard of care and expectations when an architect provides security services. When architects offer security evaluation and planning services, it

What to Look for in a Security Consultant

Broad-based in-depth knowledge and practical experience in

- Loss prevention strategy
- Current surveillance technology
- Emergency planning
- Physical security
- Protection of sensitive information
- Ability to conduct expert-level threat, vulnerability, and risk analyses
- Expert-level knowledge of internal and external safety and security issues
- Substantial experience in identifying problem areas and causal factors
- Professional experience in developing state-of-the-art programs capable of
- Protecting human, financial, and physical assets
- Preventing losses
- Enhancing the safety of the work environment
- Ability to collaborate with senior executives and design professionals
- Knowledge of planning, programming, and managing security operations
- Knowledge of criminal law and the criminal justice system to identify legal implications associated with security and safety programs

is important for them to obtain a basic understanding of the subject, carefully qualify their consultants, and address issues of scope, disclaimers, and other factors that may affect professional liability.

Architects providing security services may use a forthcoming AIA scope document for security evaluation and planning services, which can be attached to AIA Document B141-1997, Standard Form of Agreement Between Owner and Architect. (This document will contain language stating that the architect cannot guarantee or warrant that security planning and evaluation recommendations will eliminate identified risks or preclude damage or injury caused by criminal or terrorist actions.)

When engaging a security consultant, the architect may use one of several AIA C-series documents, including C141-1997, Standard Form of Agreement Between Architect and Consultant; C142-1997, Abbreviated Standard Form of Agreement Between Architect and Consultant; and C727-1992, Standard Form of Agreement Between Architect and Consultant for Special Services.

When a client engages a security consultant directly, the architect should verify the consultant's role and responsibilities in order to allocate adequate time in the design process to review and coordinate security-related information provided by the client's consultant.

PROCESS

Security assessments analyze actual, potential, and foreseeable threats to identify which combination of security measures can be applied to achieve the level of protection desired. The appropriate level of security for a particular building depends on the nature of the assets housed, the kinds of threats perceived, and the client's expectations. The actual or potential risks identified are balanced with the desires and needs of the owners in reaching a design solution.

The major components of a security assessment include asset analysis, threat analysis, vulnerability analysis, risk analysis, and identification of security measures. Tasks within these increments can vary in scope and detail depending on specific project requirements.

Asset Analysis

Asset analysis involves identifying a client's assets and assigning a value to them. In our culture, human life is valued above all other considerations. Consequently, for moral and ethical reasons, the protection of people is preeminent above all others. Practically, clients need to protect other valuable commodities that directly or indirectly contribute to their success. These include physical assets such as buildings and related infrastructure; business and personal property, including telecommunication and electronic data equipment and peripherals; and intellectual property such as proprietary information pertaining to business processes, financial status, strategic plans, personnel information, and other sensitive data.

Identifying and valuing assets is a complex process. A practical approach to asset analysis, at a minimum, should include the following steps:

- List the client's specific assets, including people, money and other negotiable instruments or commodities, information, equipment, processes, finished and unfinished goods, buildings and facilities, and other, intangible assets.
- Categorize the assets as critical (essential to the operation) or secondary (replaceable).
- Identify physical or operational assets essential to the overall operation of the enterprise.
- Determine the nature, sensitivity, and scope of the data or information the client must protect to ensure business continuity.
- Assign a criticality rating to each asset that is essential to the operation. To ensure an objective evaluation, document the monetary, intrinsic, operational, regulatory, intangible, and personal value of these critical assets.

Threat Analysis

Identifying actual, foreseeable, probable, and possible threats makes it possible to develop specific security measures. Other than natural catastrophes, most man-made threats can be grouped into three major categories: deliberate and malicious, accidental and incidental, and negligent and ignorant.

Architects and security practitioners work to develop adequate security measures to deal with deliberate and malicious acts. Their research and analytical efforts are designed to define and evaluate the intent, motivation, and possible tactics of those who may carry out identified threats. The process involves gathering historical data about hostile events and evaluating information relevant to threats against the facility. Some questions to be answered in a threat analysis might include the following: What factors about the company or organization invite potential hostility? How conspicuous is the building? How vulnerable does the building appear? What political event(s) may generate new hostilities? Have facilities like this been targets in the past?

Threats can be categorized as actual, foreseeable, or probable. Development of strategies to counter identified threats is based on documentation of similar events; identification of the degree of exposure of a building or project; determination of potential opportunities for carrying out the threat; and profiles of adversarial categories based on known objectives, organizations, operations, behavior, and resources.

Also to be considered are the threats of low-probability, high-consequence events, which cannot be statistically predicted. These threats represent a worst-possible-case scenario for which it would be prohibitively expensive and most likely unjustifiable to plan for all contingencies. For example, terrorists could detonate a nuclear device in a major urban area or unleash an exceptionally lethal quantity of chemical or biological agent where casualties could run into the tens of thousands. In these scenarios, neither time, location, nor probability can be established with any degree of accuracy, and planning for them on an individual project level is nearly impossible.

Vulnerability Analysis

Identifying actual or potential vulnerabilities requires a combination of practical experience and professional knowledge of security matters. However, vulnerability analysis also demands the ability to realistically anticipate all contingencies and an appreciation of the owner's desires and the architect's efforts to meet them. In the end, the goal is to identify how individuals could exploit specific weaknesses of the project or its location.

Identifying the vulnerabilities of a project, whether an existing building or a proposed one, involves a systematic approach to analyzing the effectiveness of the overall (actual or anticipated) security strategy at the facility. The process includes the following steps:

- Determining the objectives of the facility's physical protection system
- Identifying physical protection elements in place (or proposed) to prevent or mitigate security concerns
- Comparing system design to the objectives in a systematic, quantitative manner to determine if the physical protection system is effective and acceptable for the facility

In the context of identifying vulnerabilities, the primary purpose of a security assessment is to evaluate the security posture of a facility. The scope of this effort will include characterizing the facility and its operation, defining the threat, identifying security targets, determining security system objectives, identifying existing or proposed physical protection system elements, and analyzing the effectiveness of the security system, including identifying any deficiencies.

Risk Analysis

Simply put, the process of risk analysis is a consideration of different social, criminal, and environmental problems and the relative risk they pose to human life, asset protec-

tion, institutional reputation, and business continuity at the client's project site. The results of such an analysis typically take the shape of a list on which some risks are ranked as higher than others. The process of ranking risks provides a conceptual framework for decision-making based on information about threats, risk reduction opportunities, and economic and societal consequences of various threat reduction and risk management strategies.

An approach to carrying out a risk analysis could include the following:

- Identifying and ranking of the relative risks posed by social, criminal, political, and environmental problems based on explicit scientific criteria
- Identifying uncertainties and data quality issues associated with the relative risks of ranked threats
- Evaluating identified threats and determining whether they require near-term or long-term strategies
- Analyzing risk reduction options to create a comprehensive comparison of them, including cost-benefit implications for each

To assess and rank risk reduction measures, each is evaluated according to how it contributes to achieving the desired level of protection. Decision makers can use the results to establish priorities and make informed decisions about the available options.

Level of Protection

The security assessment steps of asset, threat, vulnerability, and risk analyses provide the basis for defining a desired level of security protection. Varying levels of protection may require different combinations of security strategies and measures. Architectural, technological, and operational elements are generally combined to provide the designated level of protection. Using basic security design concepts, the architect's task will be to incorporate these elements into a design that also responds to other functional requirements.

The accompanying chart lists some of the many opportunities and measures that can be used to enhance building security using physical, technological, and operational strategies. Each measure should be viewed and considered with respect to how it may affect other security measures as well as other design factors.

Documentation of Findings

When the architect provides the client with a security assessment report, it may be a stand-alone product or it may be part of a programming report if programming services are provided. In either case, the report communicates information the client and architect can use to integrate security into the decision-making process during design. Sometimes the report may be supplemented with videotapes, compact disks, photographs, charts, and diagrams. Parts of the report would typically include an executive summary; a statement of goals and objectives; a description of activities and methods used; descriptions of the findings of asset, threat, vulnerability, and risk analyses; and a section describing strategies and measures for application in design.

OUTLOOK ON SECURITY PLANNING

There is little evidence that the future will be less complex or that conflicts will fade away. Regrettably, the facts suggest otherwise. The demand for security evaluation and planning services is likely to be more substantial in the future as building owners look for a rational basis for investing in security protection. Moreover, even after design is completed and a facility is operational, changing conditions will call for periodic reevaluation of risks. This need will be driven by changes in assigned assets, perceived threats, and opportunities for asset compromise based on new exposures or outdated or aging security measures. To address these changes, subsequent security assessments may be conducted independently or as part of a more comprehensive postoccupancy evaluation.

Strategies

Physical Technological Operational

To enhance access control by

- Securing the site perimeter
- Using barriers to prevent passage of vehicles
- Minimizing number of entrances into building
- Securing vulnerable openings (e.g., doors, first-floor windows, etc.)
- Installing electronic access systems (e.g., parking, elevators, etc.)
- Securing critical functions (e.g., IT, mechanical rooms, etc.)

To enhance surveillance by

- Placing windows and doors to allow for good visibility
- Avoiding spaces that permit concealment
- Defining public versus private interior zones
- Avoiding blocking lines of sight with fencing and landscaping
- Locating public areas (e.g., restrooms) where they can be easily observed
- Designing lighting to reinforce natural surveillance
- Installing intrusion devices and video systems

To mitigate blast effects by

- Designing structural systems to prevent or delay building collapse
- Using building configurations to better resist blast shock waves
- Maximizing distances between parking and buildings
- Sizing and locating window areas with detonation points in mind
- Using blast- or ballistic-resistant glazing
- Increasing strength of exterior cladding and nonstructural elements
- Avoiding exterior ornamentation that can break away
- Preparing evacuation procedures for bomb attacks

To provide biochemical protection by

- Elevating fresh-air intakes
- Preventing unauthorized access to fresh-air intakes
- Protecting incoming utilities
- Applying external air filtration and overpressurization techniques
- Using internal air filtration technologies
- Securing vulnerable areas (e.g., mechanical rooms, storage, etc.)
- Establishing mail-handling protocols and procedures
- Establishing emergency plans for biochemical attacks

Source: AIA, *Building Security Through Design: A Primer for Architects, Design Professionals, and Their Clients* (2001)

“Security Evaluation and Planning” was originally published in *The Architect’s Handbook of Professional Practice, Update 2003*, ©2003 by the American Institute of Architects, published by John Wiley & Sons, Inc.

The AIA provides a contract document designed especially for these types of architectural services. The AIA suggests a two-part agreement:

B102–2007, Standard Form of Agreement Between Owner and Architect without a Predefined Scope of Architect’s Services provides terms and conditions only.

B206–2007, Standard Form of Architect’s Services: Security Evaluation and Planning provides the architect’s scope of services only.

Together they equal a complete owner-architect agreement.

AIA Document B206™–2007 establishes duties and responsibilities where the architect provides services for projects that require greater security features and protection than would normally be incorporated into a building design. This scope requires the architect to identify and analyze the threats to a facility, survey the facility with respect to those threats, and prepare a risk assessment report. Following the owner’s approval of the report, the architect prepares design documents and a security report. B206–2007 is a scope of services document only and may not be used as a stand-alone owner/architect agreement. NOTE: B206–2007 replaces AIA Document B206™–2004 (expired May 31, 2009).

For more information about AIA Contract Documents, visit www.aia.org/contractdocs/about

May 2011 The American Institute of Architects