A review of recent guidance documents produced to help reduce the vulnerability of buildings to airborne chemical and biological attacks.

The 9/11 attacks and subsequent anthrax mailings were vivid demonstrations of the potential consequences of terrorist attacks on buildings and their occupants. In the wake of these events, government, construction industry, and facilities management organizations initiated efforts to identify and disseminate guidance for making buildings less vulnerable to terrorist threats. The result of these efforts is a growing collection of documents that, with varying degrees of detail, address security of existing and new buildings from pre-construction planning through post-incident response.

This overview of recent building security guidance focuses on recommendations for reducing the impact of airborne chemical and biological (CB) attacks through planning, design, and operation. Responsibility for implementing this guidance falls mainly upon architects and the professionals who design, construct, and operate heating, ventilating, and air conditioning (HVAC) systems. The fundamental challenge to these groups is to adopt security as a design parameter in addition to comfort, health, energy conservation, and other more routine considerations.

**Sources and Scope of Guidance**

The sidebar lists the primary documents available prior to September 2001 and the most significant documents issued or revised since then. Before the Fall 2001 anthrax incidents, guidance on protection of buildings and their occupants from terrorist attacks was prepared mainly by government agencies, directed
mainly at designers of government facilities, and not widely disseminated. Most of these documents focused on the most common types of incidents of the time, such as bombings and kidnappings, which could be addressed effectively through site security (CETS 1988; GSA 2000a, 2000b). A 1986 U.S. Army technical manual (DoA 1986) provides HVAC design guidance for hardened underground facilities, but focuses on the application of specialized military particulate and gas filters not likely to be found in civilian applications. Post 9/11 guidance has been published by a broader spectrum of organizations, addresses the general building stock, and is intended for wide distribution.

The points of view represented in this collection of documents cover the full range of building professions. In addition to government agencies such as the Department of Defense and national laboratories, organizations representing architects (AIA), HVAC engineers (ASHRAE), and facility managers (IFMA) each have produced at least one significant security document within the last two years. Because they have differing scopes and are written from different points of view, the various documents classify security measures somewhat differently. Topics covered in most of the published guidance include:

**Risk management**—the process by which a building owner determines what protective measures are justified.

**What not to do**—cautions about making changes to a building or its operation that
may do more harm than good.

Physical security—building modifications and security practices to reduce the likelihood that a CB agent will enter a building.

Protective technology—building and mechanical system modifications to minimize the effects of an attack.

Protective action—planning and strategies for sheltering, evacuation, and operation of HVAC systems to minimize the effects of an attack.

Maintenance and commissioning—improving resistance to CB attacks by ensuring proper system operation.

The referenced documents, cumulatively totaling hundreds of pages, address these areas in considerable detail. This summary provides only an introduction to the content of these documents, which interested readers should obtain and study. All of the guidance reviewed here is readily available in print or electronic form, most of it at no cost.

RISK MANAGEMENT

ASHRAE (2003) defines risk management as “a systematic approach to the discovery and treatment of risks facing an organization or facility. The goal is to help objectively state, document, and rank risk, and prepare a plan for implementation.”

Both AIA (2001) and ASHRAE (2003) stress the use of risk management techniques to identify appropriate countermeasures for a particular situation. Although these documents, particularly the ASHRAE report, discuss specific measures that can be implemented, they are fundamentally about the process that the owner and owners’ professionals should apply in crafting a security plan.

AIA (2001) defines baseline building security as “the sum of access control, surveillance, and response.” Enhanced security in response to increased perception of risk adds building hardening and biochemical protection to these other basic measures. The AIA guidance breaks risk assessment into analysis of assets to be protected, threats (including reasons why a facility would invite attack and possible hostile actions), and building vulnerabilities (defined as anything that can be exploited to carry out a threat).

ASHRAE (2003) describes risk management as a four-step process encompassing risk analysis, risk treatment planning, risk treatment plan evaluation, and re-evaluation after implementation. Risk analysis as defined by ASHRAE is a six-step process, similar to the risk assessment process described by AIA: determining the organization’s level of exposure, identifying the risk, estimating the probability of risk occurrence, determining the value of the loss, ranking risks, and identifying the building’s vulnerabilities.

NIOSH (2002), in an interim document intended to provide guidance on security measures that could be implemented in the short-term, does not discuss risk management, but begins by admonishing owners to “know their buildings.” The first recommendation of the initial guidance published by ASHRAE’s Presidential Study Group (ASHRAE 2002), is “understand your building.” In a similar vein, the starting point for the U.S. Army Corps of Engineers (USACE) draft document (USACE 2001) is a discussion of how to determine a building’s protective capability. These sources reinforce the need for vulnerability analysis noted by both the 2003 ASHRAE report and AIA.

Guidance from IFMA (2002) concisely reviews vulnerability and physical security assessment and provides checklists for dealing with a range of terrorist threats. These include bombs, biological agents, chemical agents, civil disturbances, kidnappings, fire, and power outages. Like ASHRAE, IFMA emphasizes the importance of a structured decision-making process and the development of effective plans that anticipate a spectrum of hazards, not just a CB attack.

An older, but still very relevant and informative document addressing risk management is the 1988 National Research Council’s Commission on Engineering and Technical Systems report on protection of federal office buildings (CETS 1988). In addition to describing the risk management process, the report provides checklists for threat and vulnerability analysis that provide a good starting point for a tailored site and building evaluation. Threat analysis checklist items include factors such as the conspicuousness of the building, activities in the building that invite hostility, and a survey of individuals with information relevant to an attack. Vulnerability assessment includes items such as review of site topography, vehicle access, and mail handling areas. While CB weapon attacks were not foremost in the mind of the authors of this report, it retains its timeliness in the present environment.

The minimum anti-terrorism standards of the Department of Defense (DoD 2002a) provide guidance for the securing of government facilities that is both broad and specific. The philosophy on which the document is based is “that comprehensive protection against the range of possible threats may be cost prohibitive, but that an appropriate level of protection can be provided for all DoD personnel at
a reasonable cost.” Specific recommendations are generally consistent with the guidance found in other documents. What is particularly noteworthy about the DoD standards is the use of a classification scheme to describe levels of protection that are then applied to various types of facilities on the basis of risk.

WHAT NOT TO DO
Both NIOSH (2002) and ASHRAE (2002, 2003) pointedly caution building owners and engineers against making changes that may have unforeseen adverse effects on normal building operation. The 2003 ASHRAE report notes that the great majority of operating hours for most buildings are under normal conditions and that intentional threats to buildings are only one of a spectrum of possible incidents, such as fire, earthquake, or other natural disasters, that may place building occupants and contents in jeopardy. Most importantly, an enhanced security building must still meet or exceed the indoor environment and safety standards that apply to any other building.

Security measures with adverse consequences for building operation include sealing outdoor air intakes, making modifications to HVAC systems without understanding their effects, and altering fire protection and other life safety systems. A frequently cited example of an HVAC system change with negative consequences for normal building operation is a high-efficiency filter upgrade that permanently increases fan energy use and/or reduces supply air flow rate.

PHYSICAL SECURITY
Physical security is the prevention of access to facilities or vulnerable parts of facilities. Pre-9/11 documents on protection of facilities from terrorism (e.g., GSA 1999, 2000a, 2000b) focus mainly on physical security: site considerations, access limitations, and hardening of envelopes. Because protection of government facilities from armed attacks and explosives has always been a concern, it is the most extensively covered aspect of security.

The most publicized physical security measure relating to prevention of CB attacks is protection of outdoor air intakes to prevent their use as a point of introduction for a CB agent. Elevation of outdoor air intakes is recommended by

<table>
<thead>
<tr>
<th>Pre 9/11/01 Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Department of the Army (DoA) Heating, Ventilation and Air Conditioning of Hardened Facilities (1986)</td>
</tr>
<tr>
<td>• U.S. Army Corps of Engineers (USACE) Design of Collective Protection Shelters to Resist Chemical, Biological, and Radiological (CBR) Agents (1999)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Post 9/11/01 Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>• International Facility Management Association (IFMA) Addressing the Threat of Terrorism: Guidelines for Prevention and Response (2002)</td>
</tr>
<tr>
<td>• National Air Filtration Association (NAFA) Position Statement on Bio-Terrorism (2001)</td>
</tr>
<tr>
<td>• U.S. Army Corps of Engineers (USACE) Protecting Buildings and their Occupants from Airborne Hazards (draft 2001)</td>
</tr>
</tbody>
</table>
Another clear impression from current guidance is that building security lies not in a single silver bullet technology, but rather, in the layering of multiple modes of protection.

(NIOSH 2002).

Secure access to HVAC and other building system controls is recommended by Lawrence Berkeley National Laboratory (LBNL 2003) and ASHRAE (2003). This is important because of the potential for manipulation of HVAC controls by unqualified persons, or worse, terrorists, which could worsen the impact of a CB attack.

HVAC design features intended to inhibit the spread of airborne hazards include the use of ducted returns (NIOSH 2002) and compartmentalized zoning (USACE 2001, ASHRAE 2003). Other measures include securing mechanical rooms, having secure return air grilles, restricting roof access, and similar tactics.

Restricting access to building information that could aid in the planning of an attack is also recommended. The ASHRAE (2003) report provides a particularly thorough list of security vulnerabilities that should be evaluated and eliminated.

PROTECTIVE TECHNOLOGY

Positive pressurization of buildings relative to the outdoors is recommended in all documents that deal with HVAC system design. Although it may have little effect on an indoor release, it is clearly beneficial as a means of limiting vulnerability to outdoor releases. Zoned pressurization, when feasible, may assist in the containment of an indoor release and protection of egress paths. Several guidance documents note the importance of envelope tightness for preventing entry of airborne hazards and their control by pressurization strategies (NIOSH 2002, ASHRAE 2003).

Shelter in-place responses to CB attacks and other hazardous releases require that buildings have areas that can be isolated, at least for a period of time, from contaminated surrounding spaces. The 2002 preliminary ASHRAE report concludes that areas of refuge are not economically viable in most cases and recommends containment of releases and protection of egresses as more practical investments in security. However, both ASHRAE reports acknowledge the potential usefulness of refuge areas if they are available. Evaluation of the effectiveness of shelter in-place approaches to protection against outdoor chemical releases and further references are given in a report from the National Institute for Chemical Studies (NICS 2001).

Although written from a military perspective, the USACE technical letter on design of collective protection shelters (USACE 1999) contains detailed criteria that could be useful in the design of civilian refuge areas, including discussion of requirements for envelope leakage rates, filtration systems, and pressurization. The USACE collective protection guidance defines three classes of shelter. Class I shelters, designed for longer-term sheltering during large-scale, long-duration releases, have chemical/biological/radiological (CBR) filtration and over-pressure systems that can function in a 25 mph wind. An airlock is required in order to maintain the required 75 Pa pressurization. Class II shelters have CBR filtration without overpressure and are designed for short-term sheltering from events like a small-scale CBR release in a terrorist attack. Design pressurization for a Class II shelter is 5 Pa. Class III shelters offer short-term passive protection by shutting off ventilation and closing building openings, and are applicable to releases such as industrial accidents.

Guidance documents to date have taken an understandably conservative stance on air cleaning technology. Filtration, and primarily particulate air filtration, is the only approach that is discussed in detail and recommended for short-term implementation. Other air cleaning technologies directed at inactivation of biological agents, such as ultraviolet germicidal irradiation or photocatalytic oxidation, are viewed as lacking sufficient reliability or proof of efficacy to warrant an endorsement at present. A range of filtration options is discussed, from upgrading of existing HVAC filtration systems (NAFA 2001; USACE 2001; NIOSH 2002, 2003; ASHRAE 2003) to addition of separate filtration units. Both full-flow and side-stream filtration are options that an owner or engineer should consider.

ASHRAE (2003) recommends using filters with the highest MERV rating (ASHRAE 1999) that is physically feasible (i.e., will not adversely affect normal building operation). The NAFA (2001) position statement suggests that filtration should be upgraded to the highest MERV rating possible within an
HVAC system’s capability and that gas phase filtration should be considered when there is perceived risk of attacks with chemical agents. The USACE (2001) draft guidance makes specific reference only to HEPA and carbon filters.

One of the most recent additions to the security literature is the NIOSH guide on filtration and air cleaning (NIOSH 2003). It presents a far more detailed consideration of filtration options than the earlier NIOSH guidance, including a non-specialist introduction to filtration theory, discussion of standards, application consideration, and economics. Unlike the other documents addressing air cleaning, the NIOSH guide acknowledges the possibility that emerging technologies may be suitable for security applications. However, NIOSH declines to name any specific technologies in this category and instead gives guidelines for the evaluation of prospective new technologies by potential users. A particularly pertinent suggestion is to obtain relevant performance data for an application and be sure to understand how and by whom it was obtained.

The NIOSH air cleaning guide includes an important observation that should be noted by any owner operating under typical budget constraints: the measures described in the document “also provide the side benefits of improved HVAC efficiency, increased building cleanliness, limited effects from accidental releases, and generally improved air quality.” Given the low likelihood of an attack on most facilities noted by several of the other guidance documents (IFMA 2002, ASHRAE 2003), this should be a significant factor in decisions to invest in enhanced filtration or other air cleaning technology for the sake of security. A paper prepared by Lawrence Berkeley National Laboratory (Harris, et al. 2002) concludes that, for government buildings, the addition of security features should be viewed as an opportunity to improve both air quality and energy efficiency.

**PROTECTIVE ACTION**

For the purpose of this discussion, protective action includes all manual and automatic responses to an identified CB attack and excludes systems that are in operation continuously, for example, enhanced filtration. The effect of protective actions may be to facilitate evacuation or sheltering in-place and/or to collect, destroy, or purge airborne CB agents.

An important aspect of any protective action is alerting and informing building occupants. This aspect of response to an incident is addressed in the Department of Defense Unified Facilities Criteria for mass notification systems (DoD 2002b). This document provides detailed guidance on how to comply with mass notification requirements given in the DoD minimum anti-terrorism standards (DoD 2002a).

ASHRAE (2003) notes that “sensors, monitors, and other means of forewarning are not presently available or reliable for many contaminants. Therefore, strategies other than feedback control are relied upon today and for the foreseeable future.” In other words, until affordable sensor technology is available, the initiation of protective action will be manually initiated, even if the subsequent system response is automatically controlled.

ASHRAE guidance asserts the need for “a control sequence continuum from normal operations to effective responsiveness during the occurrence of an extraordinary incident.” Two possible responses to an extraordinary incident such as a CB attack are described; the choice between them depending on whether or not the building HVAC system has protective features. When protective features are not available, shutting down the system is the only alternative to normal operation. However, because this may increase exposure to the agent if it is being released internally, conditions under which a shut down would occur should be carefully reviewed. When protective measures are available during an internal release, HVAC controls should isolate the zone and start any special air-cleaning components. Controls should also operate intake and exhaust dampers to regulate building pressures. During an external release of a known agent, with protective measures in place for that agent, the system should continue to run. When there is doubt regarding either the agent or the efficacy of countermeasures, the system should be shut down.

Guidance from USACE (2001) recommends using the ventilation system and smoke-control fans for pressurization purging in a manner appropriate to the type of release. As in the case of ASHRAE’s recommendations, the response recommended by USACE depends on whether the release is internal or external. Purging is ruled out for external releases or when a hazardous material is identified indoors prior to or immediately after release. Purging is recommended for indoor releases that have already spread through the building. In other cases, use of...
air distribution systems to contain a release to facilitate evacuation or sheltering in-place is advised.

NIOSH (2002) recommends evaluating HVAC control options and provides general advice on response strategies. It is noted that shut down may be most appropriate for outdoor releases and that interior pressurization may be useful in other circumstances to protect egress and prevent spreading of agents. Low-leakage fast-acting outdoor air dampers are recommended to minimize spread of agents through HVAC distribution systems whether they are operating or shut down. The need to design control responses in consultation with qualified professionals is emphasized, as is the importance of training staff responsible for carrying out a response plan involving the HVAC system.

The Lawrence Berkeley National Laboratory guidance (LBNL 2003) describes a range of responses, depending on whether a release is indoor or outdoor, chemical or biological. For example, for an indoor biological release, the recommended actions are to limit the number of people exposed, close HVAC dampers and turn off all fans, pressurize stairwells with outside air, and segregate exposed people. For each recommended measure, a justification and discussion is provided. For indoor chemical releases, three types of HVAC control response to an identified release are described: continue normal HVAC operation (default), set systems to maximum outdoor air (better), and perform “sophisticated” HVAC manipulations, such as pressurization to isolate contaminated areas (best). The authors note their recommendations are not entirely consistent with other sources, specifically USACE (2001). They also indicate that some of the recommendations remain under review and may be modified as a result of further study.

MAINTENANCE AND COMMISSIONING

Many of the cited references recommend review of building and HVAC system performance from the perspective of vulnerability to CB attacks (ASHRAE 2003; NIOSH 2002, 2003). Review of filter installation, sealing of unintentional leakage in the building envelope, and other maintenance activities can contribute to better performance of a building subjected to an attack. Clearly, protective systems cannot be reliable unless properly installed and maintained. In addition, ASHRAE (2003) emphasizes the need for commissioning and re-commissioning of systems to maximize the likelihood of proper function during an extraordinary incident.

DISCUSSION

In a relatively short period of time, a wide range of organizations have produced a variety of useful guidance documents for improving the security of buildings and the response to terrorist and other threats. These documents cover security of new buildings from planning through operation and bring to the forefront the need for a risk management approach to design and operating decisions. Perhaps the clearest theme of guidance to date is that security considerations must be integrated with other design and operating criteria and that the risk of terrorist attacks must be considered in the context of the full range of hazards that can put buildings and their occupants at risk.

Another clear impression from current guidance is that building security lies not in a single silver bullet technology, but rather, in the layering of multiple modes of protection. Access and information control, HVAC and building design, and occupant training, as well as other measures, can combine to make buildings safer without making them less open or conducive to productivity.

Because of the sudden emergence of security as an issue for virtually all buildings, this guidance is understandably incomplete. The framework of risk management is thoroughly described and protective measures are identified, but full scientific and technical information necessary to implement them is not available. Two clear needs are more specific guidance on system design and better characterization of advanced air cleaning technologies. A third important void is in the area of design criteria, about which there has been little discussion and, certainly, no consensus.

The set of criteria minimally required to design protective measures consists of the agents, the manner of their release into or within a building, and the acceptable exposures. A hypothetical set of “design basis” agents might include a gaseous chemical agent of a particular toxicity, and a range of infectious agents from viruses to spores. “Design basis” releases might include an outdoor release, and both instantaneous and longer-term releases in an air handling unit or outdoor air intake, and in an occupied space. This is a complex issue, but one that needs to be addressed. Once these criteria are established, formal analyses can be constructed to assess risk and evaluate the performance of various protective actions or systems quantitatively. Similarly, there is much promising air-cleaning technology that has not been fully characterized for use in security appli-
cations. Until emerging technologies are supported by sufficient independent evidence of efficacy, their use will be inhibited.

It is expected that over time, gaps in guidance will be filled in by research and experience. A case in point is the issuance of the 2003 NIOSH filtration and air-cleaning guide following the 2002 publication of interim advice. In the near term, however, owners and engineers may find less clear guidance in the available documents than they would prefer to have. However, as the authors of the ASHRAE (2003) report note, “these limitations in our knowledge base are not a justification for the abrogation of one’s responsibility to deal with the potential risks in a building.” During the interim, it is incumbent upon owners and engineers to make the best use of their experience and judgment to deal with the challenge of security in an age of global terrorism.

REFERENCES


Inc., Atlanta, GA.


LBNL. 2003. Protecting buildings from a biological or chemical attack: actions to take before or during a release. LBNL/PUB-51959. Lawrence Berkeley National Laboratory, Berkeley, CA.


ABOUT THE AUTHOR

William P. Bahnfleth, Ph.D., P.E. is Associate Professor of Architectural Engineering and founding Director of the Indoor Environment Center (IEC) at The Pennsylvania State University. He holds a Ph.D. in Mechanical Engineering from the University of Illinois and is a Registered Professional Engineer. He teaches and conducts research in a variety of areas related to HVAC system design and operation, including indoor air quality (IAQ). His IAQ research activities in collaboration with IEC colleagues are mainly in the area of air disinfection technologies, including dilution, filtration, and ultraviolet germi-
cidal irradiation. He also investigates system-level issues in microbial control, most recently, the modeling of biological agent releases in and around buildings and their response to various control strategies. Dr. Bahnfleth is a member of the editorial advisory board of *Heating/Piping/Air Conditioning (HPAC) Engineering* magazine.