STEP 1: THREAT IDENTIFICATION AND RATING

OVERVIEW

The first step in the assessment process is to help you to identify threats that are a priority concern in your area and that may pose a risk to your assets (see Figure 1-1). The threat identification and rating process involves the following tasks:

- Identifying the threats
- Collecting information
- Determining the design basis threat
- Determining the threat rating

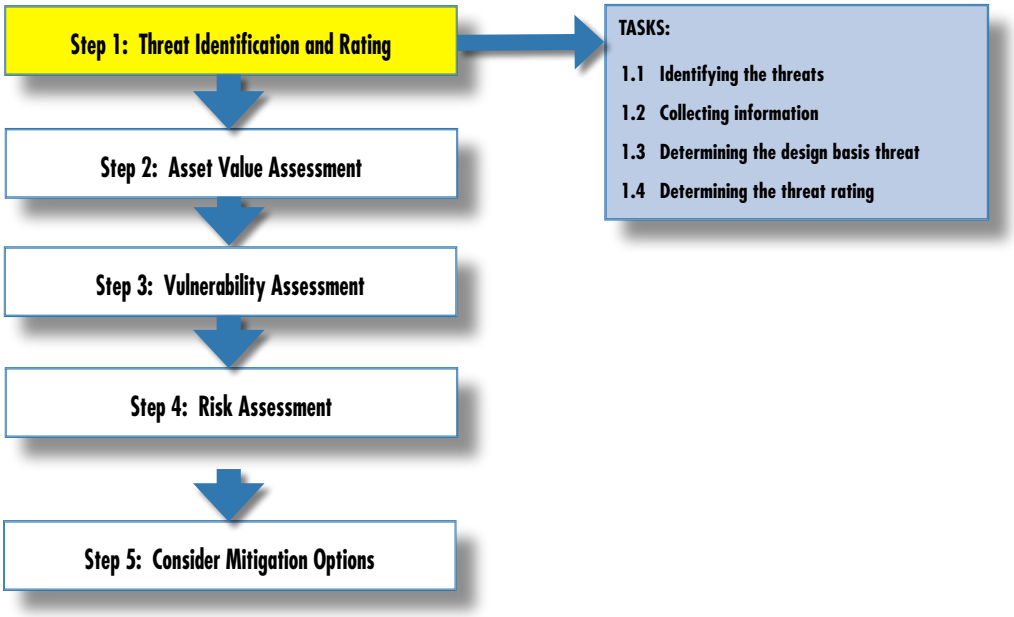

Figure 1-1 Steps and tasks

Identifying the Threats (Task 1.1)

For this document, threat is defined as any indication, circumstance, or event with the potential to cause loss of, or damage to an asset. Within the military services, the intelligence community, and law enforcement, the term "threat" is typically used to describe the design criteria for terrorism or manmade disasters. The Federal Emergency Management Agency (FEMA) and other civil agencies use the term "hazard" in several different contexts. "Natural hazard" typically refers to a natural event such as a flood, wind, or seismic disaster.

"Human-caused (or manmade) hazards" are "technological hazards" and "terrorism" and are distinct from natural hazards primarily in that they originate from human activity. "Technological hazards" (i.e., a HazMat leak from a railcar) are generally assumed to be accidental and that their consequences are unintended. (Note that protection against technological hazards can also serve for the protection against terrorist attacks.) "Terrorism" is considered an unlawful act of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

In this guide, only manmade terrorist threats will be used in the critical functions and infrastructure matrices. The importance of technological hazards is that they can become a threat if they are targets of malicious attacks.

Identifying the threats can be a difficult task. Because manmade hazards are different from other hazards such as earthquakes, floods, and hurricanes, they are difficult to predict. Many years of historical and quantitative data, and probabilities associated with the cycle, duration, and magnitude of natural hazards exist. The fact that data for manmade hazards are scarce and that the magnitude and recurrence of terrorist attacks are almost unpredictable makes the determination of a particular threat for any particular site or building difficult and largely subjective.

With any terrorist threats, it is important to understand who the people are with the intent to cause harm. The aggressors seek publicity for their cause, monetary gain (in some instances), or political gain through their actions. These actions include injuring or killing people; destroying or damaging facilities, property, equipment, or resources; or stealing equipment, material, or information. In some cases, the threat may originate from more than one group, with differing methods and motives.

Aggressor tactics run the gamut: moving vehicle bombs; stationary vehicle bombs; bombs delivered by persons (suicide bombers); exterior attacks (thrown objects like rocks, Molotov cocktails, hand grenades, or hand-placed bombs); attack weapons (rocket propelled grenades, light antitank weapons, etc.); ballistic attacks (small arms handled by one individual); covert entries (gaining entry by false credentials or circumventing security with or without weapons); mail bombs (delivered to individuals); supply bombs (larger bombs processed through shipping departments); airborne contamination (chemical, biological, or radiological [CBR] agents used to contaminate the air supply of a building); and waterborne contamination (CBR agents injected into the water supply).

Domestic terrorism refers to activities that involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any state; appear to be intended to intimidate or coerce a civilian population; to influence the policy of a government by mass destruction, assassination, or kidnapping; and occur primarily within the territorial jurisdiction of the United States.

International terrorism involves violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any state. These acts appear to be intended to intimidate or coerce a civilian population; influence the policy of a government by intimidation or coercion; affect the conduct of a government by mass destruction, assassination or kidnapping; and occur primarily outside the territorial jurisdiction of the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum. Totals for international terrorism in 1998-2003 are shown by regions in Figure 1-2.

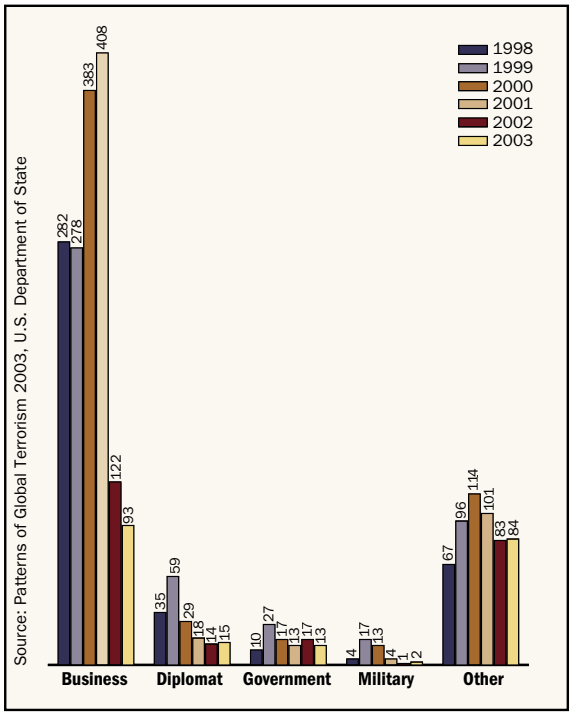

Figure 1-2 Total international attacks by region, 1998-2003

Explosive Blast Weapons

Two parameters are used to define the explosive blast design threat: the weapon size, measured in equivalent pounds of trinitrotoluene (TNT), and the stand-off. The stand-off is the distance measured from the center of gravity of the charge to the component of interest.

Figures 1-3, 1-4, and Table 1-1 illustrate these principles. Figure 1-3 shows an example of a blast range-to-effect chart that indicates the distance or stand-off to which a given size bomb will produce a given effect. Table 1-1 is a quick reference chart that provides recommended evacuation distances for a given explosive weight. Figure 1-4 provides a quick method for predicting the expected overpressure (expressed in pounds per square inch or psi) on a building for a specific explosive weight and stand-off distance. For additional information on overpressure and blast effects, see FEMA 426 and 427.

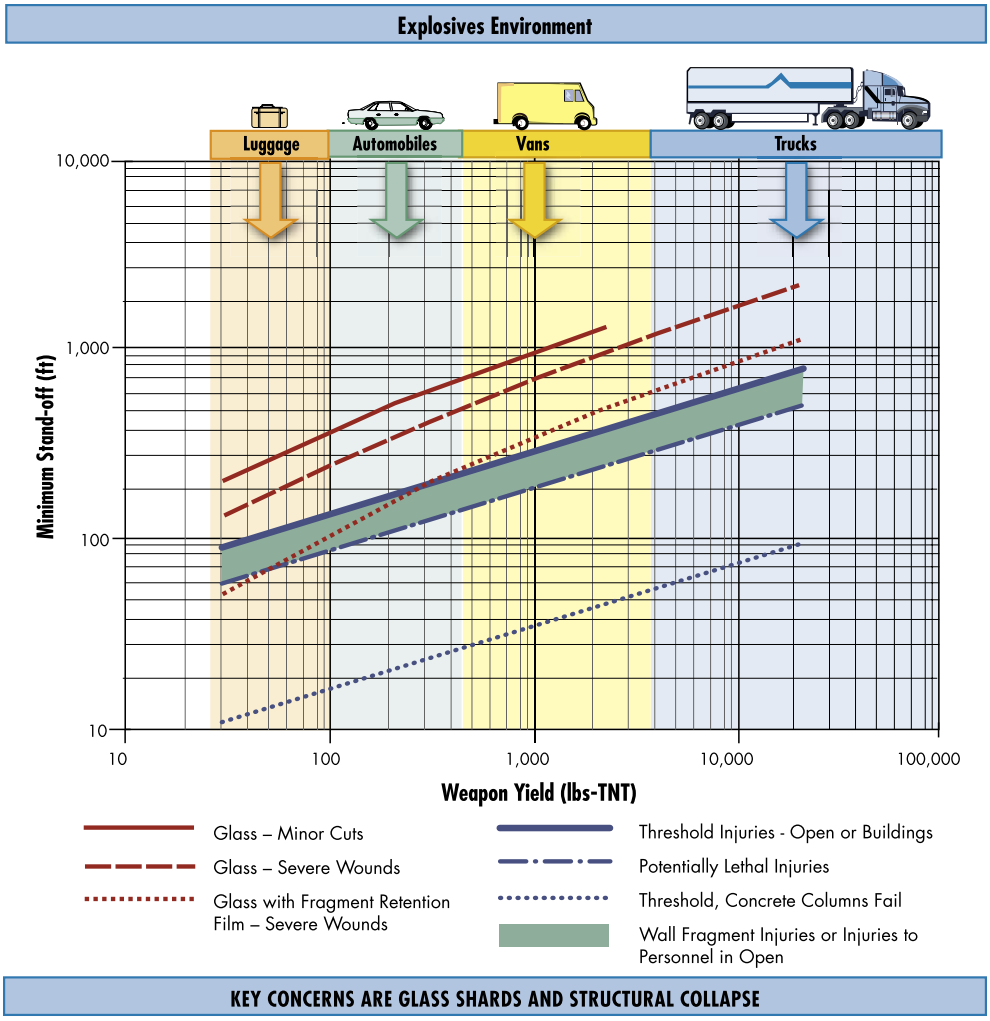

Figure 1-3 Explosive environments - blast range to effect

Table 1-1 Explosive Evacuation Distance

	Threat Description	Explosive Mass[1] (TNT Equivalent)	Building Evacuation Distance[2]	Outdoor Evacuation Distance[3]
High Explosives (TNT Equivalent)	Pipe Bomb	5 lbs 2.3 kg	70 ft 21 m	850 ft 259 m
	Suicide Belt	10 lbs 4.5 kg	90 ft 27 m	1,080 ft 330 m
	Suicide Vest	20 lbs 9 kg	110 ft 34 m	1,360 ft 415 m
	Briefcase/Suitcase Bomb	50 lbs 23 kg	150 ft 46 m	1,850 ft 564 m
	Compact Sedan	500 lbs 227 kg	320 ft 98 m	1,500 ft 457 m
	Sedan	1,000 lbs 454 kg	400 ft 122 m	1,750 ft 534 m
	Passenger/Cargo Van	4,000 lbs 1,814 kg	640 ft 195 m	2,750 ft 838 m
	Small Moving Van/Delivery Truck	10,000 lbs 4,536 kg	860 ft 263 m	3,750 ft 1,143 m
	Moving Van/Water Truck	30,000 lbs 13,608 kg	1,240 ft 375 m	6,500 ft 1,982 m
	Semitrailer	60,000 lbs 27,216 kg	1,570 ft 475 m	7,000 ft 2,134 m

[1]*Based on the maximum amount of material that could reasonably fit into a container or vehicle. Variations are possible.*

[2]*Governed by the ability of an unreinforced building to withstand severe damage or collapse.*

[3]*Governed by the greater of fragment throw distance or glass breakage/falling glass hazard distance. These distances can be reduced for personnel wearing ballistic protection. Note that the pipe bomb, suicide belt/vest, and briefcase/suitcase bomb are assumed to have a fragmentation characteristic that requires greater stand-off distances than an equal amount of explosives in a vehicle.*

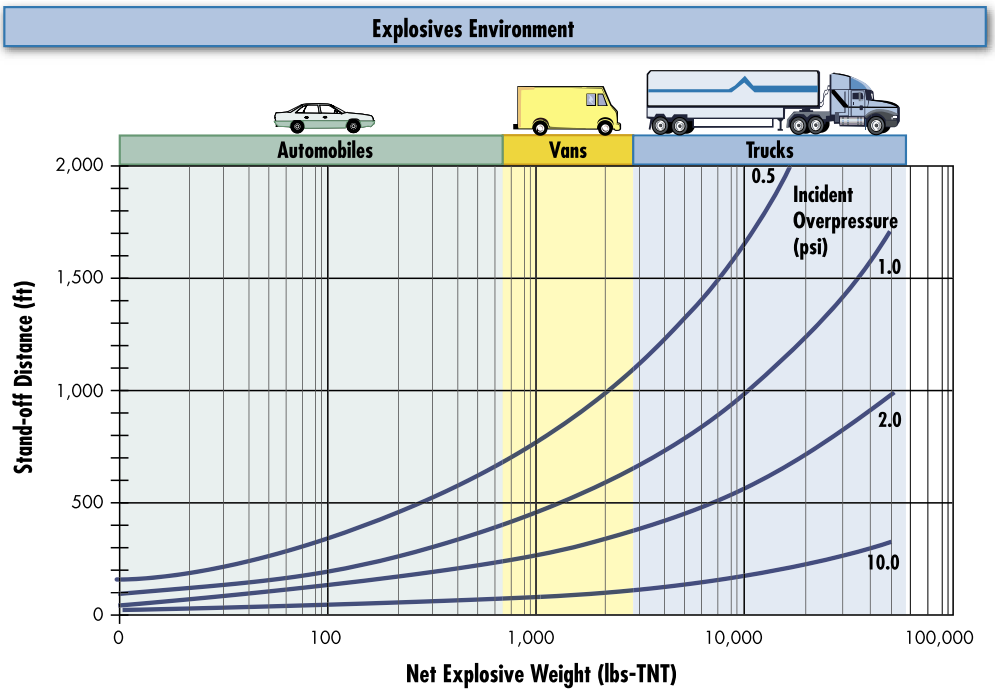

Figure 1-4 Incident overpressure as a function of stand-off distance

To put the weapon size into perspective, it should be noted that thousands of deliberate explosions occur every year within the United States, but the vast majority of them have weapon yields of less than 5 pounds. The number of large-scale vehicle weapon attacks that have used hundreds of pounds of TNT during the past 20 years is, by comparison, very small. In general, the largest credible explosive size is a function of the security measures in place. Each line of security may be thought of as a sieve, reducing the size of the weapon that may gain access. Therefore, the largest weapons are considered in totally unsecured public spaces (e.g., in a vehicle on the nearest public street), and the smallest weapons are considered in the most secured areas of the building (e.g., in a briefcase smuggled past the screening station). It should also be noted that the likely target is often not the building under consideration by the risk assessment, but a high-risk building that is nearby. Historically, more building damage has been due to collateral effects than direct attack. Based upon access to the agent, the degree of difficulty, and past experience, it can be stated that the chance of a large-scale explosive attack occurring is extremely low and that a smaller explosive attack is far more likely.

From the standpoint of structural design, the vehicle bomb is the most important consideration and has been a favorite tactic of terrorists. Ingredients for homemade bombs are easily obtained on the open market, as are the techniques for making bombs.

Vehicle bombs are able to deliver a sufficiently large quantity of explosives to cause potentially devastating structural damage. Security design intended to limit or mitigate damage from a vehicle bomb assumes that the bomb is detonated at a so-called critical location. The critical location is a function of the site, the building layout, the security measures in place, and the position of the weapon. For a vehicle bomb, the critical location is taken to be at the closest point that a vehicle can approach, assuming that all security measures are in place. This may be a parking area directly beneath the occupied building, the loading dock, the curb directly outside the facility, or at a vehicle-access control gate where inspection takes place, depending on the level of protection incorporated into the design.

Another explosive attack threat is the small bomb that is hand delivered. Small weapons can cause large damage when they are brought into vulnerable and unsecured areas of the building. Greater damage may be caused when the weapon is brought into the interior, such as the building lobby, mail room, and retail spaces. Recent events around the world make it clear that there is an increased likelihood that bombs will be delivered by persons (suicide bombers or hand carried bombs) who are willing to sacrifice their own lives. Hand-carried explosives are typically on the order of 5 to 10 pounds of TNT equivalent. However, larger charge weights, in the 50- to 100-pound TNT equivalent range, can be readily carried in rolling cases. Mail bombs are typically less than 10 pounds of TNT equivalent.

For design purposes, large-scale truck bombs typically contain 10,000 pounds or more of TNT equivalent, depending on the size and capacity of the vehicle used to deliver the weapon. Vehicle bombs that utilize vans down to small sedans typically contain 5,000 to 100 pounds of TNT equivalent, respectively. A briefcase bomb is approximately 50 pounds, and a pipe bomb is generally in the range of 5 pounds of TNT equivalent. Suicide bombers can deliver belts ranging from 10 pounds (teenagers), 15 to 20 pounds (women), and 30 to 40 pounds (men).

Chemical, Biological, and Radiological Weapons

Three parameters are used to define the CBR design basis threat: the exposure, the duration, and the concentration. Each of the CBR agents has different human effects and methods of attack.

Chemical, biological, and radiological attacks are an emerging threat and of great concern because of the large geographic area contaminated, numbers of people affected, and the high economic cost of response and recovery. The use of CBR weapons and the stated intent of terrorist groups to acquire and use the weapons increases the target set, and the weapons can affect a single building, an entire city, multiple counties, or even states.

Like explosive threats, CBR threats may be delivered externally or internally to the building. External ground-based threats may be released at a stand-off distance from the building or may be delivered directly through an air intake or other opening. Interior threats may be delivered to accessible areas such as the lobby, mailroom, loading dock, or egress route. Because there may not be an official or obvious warning prior to a CBR event, the best defense is to be alert to signs of a release occurring.

Chemical. Chemical agents are compounds with unique chemical properties that can produce lethal or damaging effects in humans, animals, and plants. Chemical agents can exist as solids, liquids, or gases, depending on temperature and pressure. Most chemical agents are liquid and can be introduced into an unprotected population relatively easily using aerosol generators, explosive devices, breaking containers, or other forms of covert dissemination. Dispersed as an aerosol or vapor, chemical agents have their greatest potential for inflicting mass casualties. There are two categories of chemicals: lethal and incapacitating. The lethal chemicals are subdivided into industrial and warfare.

Industrial chemicals are used extensively throughout the nation on a daily basis. Lethal industrial chemicals are listed as Toxic Industrial Compounds (TICs). Of concern is the use of TICs as a weapon (e.g., derailment of a chlorine tanker car), especially in the urban environment.

Chemical agents can have an immediate effect (a few seconds to a few minutes) or a delayed effect (several hours to several days). Although potentially lethal, chemical agents are difficult to deliver in lethal concentrations. Outdoors, the agents often dissipate rapidly. Chemical agents are also difficult to produce. There are six types of agents:

- Choking/lung-damaging (pulmonary) agents such as chlorine and phosgene
- Blood agents such as cyanide
- Vesicants or blister agents such as mustard
- Nerve agents such as GA (tabun), GB (sarin), GD (soman), GF (cyclohexyl sarin), and VX (phosphonothioic acid)
- Incapacitating agents such as BZ (3-quinulidinyle benzilate)

- Riot-control agents similar to Mace

Biological. Biological agents pose a serious threat because of their accessible nature and the rapid manner in which they spread. These agents are disseminated by the use of aerosols, contaminated food or water supplies, direct skin contact, or injection. Several biological agents can be adapted for use as weapons by terrorists. These agents include anthrax (sometimes found in sheep and cattle), tularemia (rabbit fever), cholera, the plague (sometimes found in prairie dog colonies), and botulism (found in improperly canned food). A biological incident will most likely be first recognized in the hospital emergency room, medical examiner's office, or within the public health community long after the terrorist attack. The consequences of such an attack may present communities with an unprecedented requirement to provide mass protective treatment to exposed populations, mass patient care, mass fatality management, and environmental health cleanup procedures and plans.

Biological agents are organisms or toxins that can kill or incapacitate people, livestock, and crops. The three basic groups of biological agents that would likely be used as weapons are bacteria, viruses, and toxins.

1. Bacteria are small free-living organisms that reproduce by simple division and are easy to grow. The diseases they produce often respond to treatment with antibiotics.

2. Viruses are organisms that require living cells in which to reproduce and are intimately dependent upon the body they infect. Viruses produce diseases that generally do not respond to antibiotics; however, antiviral drugs are sometimes effective.

3. Toxins are poisonous substances found in, and extracted from, living plants, animals, or microorganisms; some toxins can be produced or altered by chemical means. Some toxins can be treated with specific antitoxins and selected drugs.

Most biological agents are difficult to grow and maintain. Many break down quickly when exposed to sunlight and other environmental factors, while others such as anthrax spores are very long lived. They can be dispersed by spraying them in the air, or by infecting animals or humans, as well through food and water contamination.

- **Aerosols —** Biological agents are dispersed into the air as an aerosol that may drift for miles. Inhaling the agent may cause disease in people or animals.

- **Animals —** Some diseases are spread by insects and animals, such as fleas, mice, flies, and mosquitoes. Deliberately spreading diseases through livestock is also referred to as agro-terrorism.

- **Food and water contamination —** Some pathogenic organisms and toxins may persist in food and water supplies. Most microbes can be killed, and toxins deactivated, by cooking food and boiling water.

Person-to-person spread of a few infectious agents is also possible. Humans have been the source of infection for smallpox, plague, and the Lassa viruses. In a 2002 report, Public Health Assessment of Biological Terrorism Agents, the Centers for Disease Control (CDC) has classified biological agents as one of three priority categories for initial public health preparedness efforts: A, B, or C (see Table 1-2). The CDC maintains a comprehensive list of agents, diseases, and other threats at www.bt.cdc.gov/agent/index.asp.

Agents in Category A have the greatest potential for adverse public health impact with mass casualties, and most require broad-based public health preparedness efforts (e.g., improved surveillance and laboratory diagnosis and stockpiling of specific medications). Category A agents also have a moderate to high potential for large-scale dissemination or a heightened general public awareness that could cause mass public fear and civil disruption.

Most Category B agents also have some potential for large-scale dissemination with resultant illness, but generally cause less illness and death, and, therefore, would be expected to have lower medical and public health impacts. These agents also have lower general public awareness than Category A agents and require fewer special public health preparedness efforts. Agents in this category require some improvement in public health and medical awareness, surveillance, or laboratory diagnostic capabilities, but present limited additional requirements for stockpiled therapeutics beyond those identified for Category A agents. Biological agents that have undergone some development for widespread dissemination but do not otherwise meet the criteria for Category A, as well as several biological agents of concern for food and water safety, are included in this category.

Biological agents that are currently not believed to present a high bioterrorism risk to public health, but that could emerge as future threats (as scientific understanding of these agents improves) were placed in Category C.

Table 1-2: Critical Biological Agent Categories

Biological Agent(s)	Disease
Category A	
Variola major	Smallpox
Bacillus anthracis	Anthrax
Yersinia pestis	Plague
Clostridium botulinum (botulinum toxins)	Botulism
Francisella tulaensis	Tularemia
Filoviruses and Arenaviruses (e.g., Ebola virus, Lassa virus)	Viral hemorrhagic fevers
Category B	
Coxiella burnetii	Q fever
Brucella spp.	Brucellosis
Burkholderia mallei	Glanders
Burkholderia pseudomallei	Meliodosis
Alphaviruses	Encephalitis
Rickettsia prowazekii	Typhus fever
Toxins (e.g., Ricin)	Toxic syndromes
Chlamydia psittaci	Psittacosis
Food safety threats (e.g., *Salmonella spp.*)	
Water safety threats (e.g., *Vibrio cholerae*)	
Category C	
Emerging threat agents (e.g., *Nipah virus*, hantavirus)	

SOURCE: PUBLIC HEALTH ASSESSMENT OF POTENTIAL BIOLOGICAL TERRORISM AGENTS (CDC, 2002)

Nuclear and Radiological. Nuclear threat is the use, threatened use, or threatened detonation of a nuclear bomb or device. At present, there is no known instance in which any non-governmental entity has been able to obtain or produce a nuclear weapon. The most likely scenario is the detonation of a large conventional explosive that incorporates nuclear material or detonation of an explosive proximate to nuclear materials in use, storage, or transit. Of concern is the increasing frequency of shipments of radiological materials throughout the world.

Nuclear explosions can cause deadly effects: blinding light, intense heat (thermal radiation), initial nuclear radiation, blast, fires started by the heat pulse, and secondary fires caused by the destruction. They also produce radioactive particles called fallout that can be carried by wind for hundreds of miles.

Terrorist use of a radiological dispersion device (RDD) – often called ”dirty nuke” or “dirty bomb” – is considered far more likely than the use of a nuclear device. These radiological weapons are a combination of conventional explosives and radioactive material designed to scatter dangerous and sub-lethal amounts of radioactive material over a general area. Such radiological weapons appeal to terrorists because they require very little technical knowledge to build and deploy compared to that of a nuclear device. Also, these radioactive materials, used widely in medicine, agriculture, industry, and research, are much more readily available and easy to obtain compared to weapons grade uranium or plutonium.

Terrorist use of a nuclear device would probably be limited to a single smaller “suitcase” weapon. The strength of such a nuclear weapon would be in the range of the bombs used during World War II. The nature of the effects would be the same as a weapon delivered by an inter-continental missile, but the area and severity of the effects would be significantly more limited.

There is no way of knowing how much warning time there would be before an attack by a terrorist using a nuclear or radiological weapon. A surprise attack remains a possibility. The danger of a massive strategic nuclear attack on the United States involving many weapons receded with the end of the Cold War; however, some terrorists have been supported by nations that have nuclear weapons programs.

Other Threats. Other threats discussed in this manual include armed attacks, cyber attacks, high-altitude electromagnetic pulse, and high power microwave. These are discussed briefly in Table 1-3.

Table 1-3 provides selected threats that you may consider when preparing your risk assessment, some of which has not been discussed previously in this How-To Guide.

Table 1-3: Event Profiles

Threat	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Improvised Explosive Device (Bomb) - Stationary Vehicle - Moving Vehicle - Mail - Supply - Thrown - Placed - Suicide Bomber	Detonation of explosive device on or near target; via person, vehicle, or projectile.	Instantaneous; additional secondary devices may be used, lengthening the duration of the threat until the attack site is determined to be clear.	Extent of damage is determined by type and quantity of explosive. Effects generally static other than cascading consequences, incremental structural failure, etc.	Blast energy at a given stand-off is inversely proportional to the cube of the distance from the device; thus, each additional increment of stand-off provides progressively more protection. Exacerbating conditions include ease of access to target; lack of barriers/shielding; poor construction; and ease of concealment of device.
Armed Attack - Ballistics (small arms) - Stand-off Weapons (rocket propelled grenades, mortars)	Tactical assault or sniper attacks from a remote location.	Generally minutes to days.	Varies, based upon the perpetrator's intent and capabilities.	Inadequate security can allow easy access to target, easy concealment of weapons, and undetected initiation of an attack.
Chemical Agent - Blister - Blood - Choking/Lung/ Pulmonary - Incapacitating - Nerve - Riot Control/Tear Gas - Vomiting	Liquid/aerosol contaminants can be dispersed using sprayers or other aerosol generators; liquids vaporizing from puddles/ containers; or munitions.	Chemical agents may pose viable threats for hours to weeks, depending on the agent and the conditions in which it exists.	Contamination can be carried out of the initial target area by persons, vehicles, water, and wind. Chemicals may be corrosive or otherwise damaging over time if not remediated.	Air temperature can affect evaporation of aerosols. Ground temperature affects evaporation in pools of liquids. Humidity can enlarge aerosol particles, reducing the inhalation hazard. Precipitation can dilute and disperse agents, but can spread contamination. Wind can disperse vapors, but also cause target area to be dynamic. The micro-meteorological effects of buildings and terrain can alter travel and duration of agents. Shielding in the form of sheltering in place may protect people and property from harmful effects for a limited time.

Table 1-3: Event Profiles (continued)

Threat	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Biological Agent - Anthrax - Botulism - Brucellosis - Plague - Smallpox - Tularemia - Viral Hemorrhagic Fevers - Toxins (Botulinum, Ricin, Staphylococcal Enterotoxin B, T-2 Mycotoxins)	Liquid or solid contaminants can be dispersed using sprayers/aerosol generators or by point or line sources such as munitions, covert deposits, and moving sprayers. May be directed at food or water supplies.	Biological agents may pose viable threats for hours to years, depending on the agent and the conditions in which it exists.	Depending on the agent used and the effectiveness with which it is deployed, contamination can be spread via wind and water. Infection can be spread via human or animal vectors.	Altitude of release above ground can affect dispersion; sunlight is destructive to many bacteria and viruses; light to moderate winds will disperse agents, but higher winds can break up aerosol clouds; and the micro-meteorological effects of buildings and terrain can influence aerosolization and travel of agents.
Radiological Agent - Alpha - Beta - Gamma	Radioactive contaminants can be dispersed using sprayers/aerosol generators, or by point or line sources such as munitions, covert deposits, and moving sprayers.	Contaminants may remain hazardous for seconds to years, depending on material used.	Initial effects will be localized to site of attack; depending on meteorological conditions, subsequent behavior of radioactive contaminants may be dynamic.	Duration of exposure, distance from source of radiation, and the amount of shielding between source and target determine exposure to radiation.
Cyber Attacks	Electronic attack using one computer system against another.	Minutes to days.	Generally no direct effects on built environment.	Inadequate security can facilitate access to critical computer systems, allowing them to be used to conduct attacks.
High-Altitude Electromagnetic Pulse (HEMP)	An electromagnetic energy field produced in the atmosphere by the power and radiation of a nuclear explosion. It can overload computer circuitry with effects similar to, but causing damage much more swiftly than a lightning strike.	It can be induced hundreds to a few thousand kilometers from the detonation.	Affects electronic systems. There is no effect on people. It diminishes with distance, and electronic equipment that is turned off is less likely to be damaged.	To produce maximum effect, a nuclear device must explode very high in the atmosphere. Electronic equipment may be hardened by surrounding it with protective metallic shielding that routes damaging electromagnetic fields away from highly sensitive electrical components.

Table 1-3: Event Profiles (continued)

Threat	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
High Power Microwave (HPM) EMP	It is a non-nuclear radio frequency energy field. Radio frequency weapons can be hidden in an attaché case, suitcase, van, or aircraft. Energy can be focused using an antenna, or emitter, to produce effects similar to HEMP, but only within a very limited range.	An HPM weapon has a shorter possible range than HEMP, but it can induce currents large enough to melt circuitry, or it can cause equipment to fail minutes, days, or even weeks later. HPM weapons are smaller-scale, are delivered at a closer range to the intended target, and can sometimes be emitted for a longer duration.	Vulnerable systems include electronic ignition systems, radars, communications, data processing, navigation, electronic triggers of explosive devices. HPM capabilities can cause a painful burning sensation or other injury to a person directly in the path of the focused power beam, or can be fatal if a person is too close to the microwave emitter.	Very damaging to electronics within a small geographic area. A shockwave could disrupt many computers within a 1-mile range. Radio frequency weapons have ranges from tens of meters to tens of kilometers. Unlike HEMP, however, HPM radiation is composed of shorter wave forms at higher-frequencies, which make it highly effective against electronic equipment and more difficult to harden against.

Note: Cyber attack focuses on denial of service, worms, and viruses designed to attack or destroy critical infrastructure related systems such as energy management, supervisory control and data acquisition systems, security, control valves, and voice over internet protocol telephones, which are critical systems that support multiple functions and are becoming increasingly connected to the internet.

It is important to indicate that commercial buildings have been the preferred target of recent terrorist attacks. Figure 1-5 illustrates such actions. Between 1998 and 2003, 1,566 commercial facilities were struck by terrorists while only 97 government, 170 diplomat facilities, and 41 military facilities were affected during the same period.

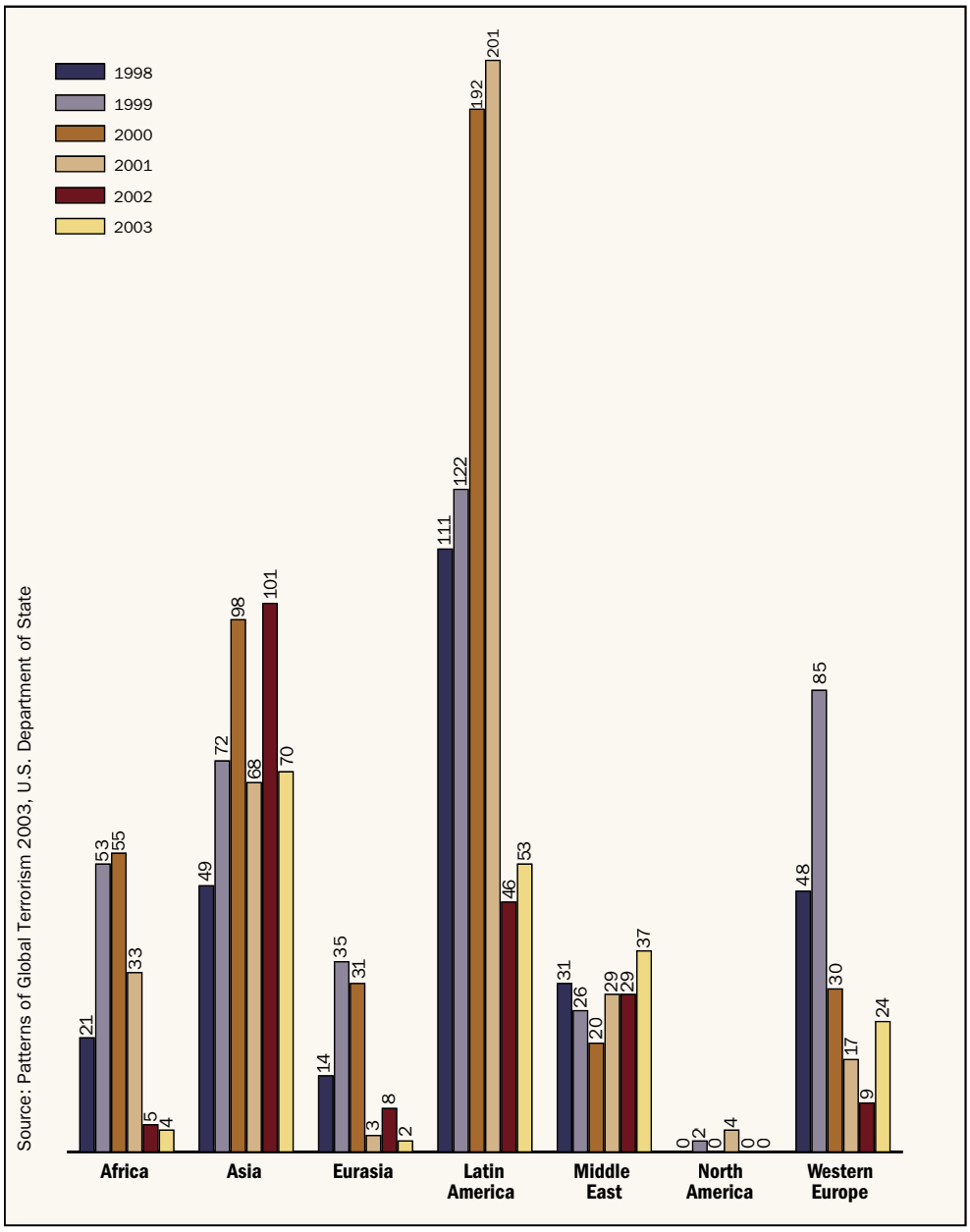

Figure 1-5 Total facilities affected by international terrorism and weapons of choice, 1998-2003

Collecting Information (Task 1.2)

When collecting information for your threat assessment, you may ask the following questions: What groups or organizations exist/are known? Do they have capability among themselves or is that capability readily obtainable locally? Do they have a history of terrorist acts and what are their tactics? What are the intentions of the aggressors against the government, commercial enterprises, industrial sectors, or individuals? Has it been determined that

targeting (planning a tactic or seeking vulnerabilities) is actually occurring or being discussed?

For technological hazards, these same questions take a different perspective. Does anything that can be a hazard (or be attacked, causing collateral damage) exist within a given distance of the building in question? What is the capability of that incident to cause harm? Is there a history of this type of accident occurring?

Many security and intelligence organizations are a good source of information and data for threat assessments. These organizations include the police department (whose jurisdiction includes the building or site), the local State police office, and the local office of the Federal Bureau of Investigation (FBI.) In many areas of the country, there are threat coordinating committees, including FBI Joint Terrorism Task Forces, that facilitate the sharing of information. In addition, the CDC, the U.S. Department of Homeland Security (DHS), and the Homeland Security Offices (HSOs) at the State level are good sources of information. For technological hazards, it is important to gather information from the local fire department and hazardous materials (HazMat) unit, Local Emergency Planning Committee (LEPC), and State Emergency Response Commission (SERC). LEPC and SERC are local and State organizations established under a U.S. Environmental Protection Agency (EPA) program. They identify critical facilities in vulnerable zones and generate emergency management plans. Additionally, most fire departments understand which industries in the local area handle the most combustible materials and the HazMat unit understands who handles materials that could have a negative impact upon people and the environment. In many jurisdictions, the HazMat unit is part of the fire department.

Other good sources of information include the Department of Homeland Security Information Analysis and Infrastructure Protection (IA/IP) Directorate and, under the Director, Central Intelligence Agency (CIA), the Terrorist Threat Integration Center (TTIC). The IA/IP Directorate and the TTIC enhance intelligence fusion to bring together all terrorist information in one place, enabling America's best intelligence analysts and investigators from multiple departments to work as a team to put together the pieces of the puzzle.

Threat information is communicated through The Homeland Security Information Network. This communications system delivers real-time interactive connectivity among State and local partners and with the DHS Homeland Security Operations Center (HSOC) through the Joint Regional Informa-

tion Exchange System (JRIES). Other DHS agencies participate through seats at the HSOC and their own operations centers, and the system will be further expanded within DHS operations. Each State and major urban area's Homeland Security Advisor and other points of contact will receive software licenses, technology, and training to participate in the information sharing and situational awareness that JRIES already brings to State and local homeland security personnel across the United States. Examples of other points of participation include State National Guard offices, Emergency Operations Centers (EOCs), and first responder and Public Safety departments.

The network significantly strengthens the flow of real-time threat information to State, local, and private sector partners at the Sensitive-but-Unclassified level (SBU), and provides a platform for communications through the classified SECRET level to State offices. The program is built upon the JRIES platform, a secure network and a suite of applications currently operating at the SBU level. Participants currently include approximately 100 organizations, including Federal agencies, States, municipalities, and other local government entities, with a significant law enforcement user base. All participating entities have a certified counterterrorism mission. Approximately 1,000 users currently have access to the system.

Determining the Design Basis Threat (Task 1.3)

Stopping a terrorist or physical attack on a building is very difficult; any building or site can be breached or destroyed. Weapons, tools, and tactics can change faster than a building can be modified against a particular threat. However, the more secure the building or site and the better the building is designed to withstand an attack, the better the odds the building will not be attacked or, if attacked, it will suffer less damage. Terrorists generally select targets that have some value as a target, such as an iconic commercial property, symbolic government building, or structure likely to inflict significant emotional or economic damage such as a shopping mall or major seaport.

The type and size of the weapons to be considered in the threat assessment are usually selected by the building stakeholders in collaboration with the Assessment Team (i.e., engineers who specialize in the design of structures to mitigate the effects of explosions - see Step 3 of this How-To Guide). The threat assessment and analysis for any building can range from a general threat scenario to a very detailed examination of specific groups, individuals, and tactics that the building may need to be designed to repel or defend against. For this How-To Guide, a simplified method has been selected to help the Assessment Team and building stakeholders to identify the primary

threats to their buildings (see Selecting Primary Threats below and Table 1-4).

It is important to indicate that there are other sophisticated methods and criteria that can be used for more detailed threat analysis, including the TM5-853 Army-Air Force Security Engineering Manual, the State of Florida HLS-CAM vulnerability and criticality matrix, the Department of Defense (DoD) CARVER process, and the FEMA 386-7 Site/Building Inherent Vulnerability Assessment Matrix. The determination of which method to be used should be left to the Assessment Team and building owners.

The methodology presented in this How-To Guide is based upon several methodologies, including some of the ones listed above. It provides a simple and straight forward approach to focus on the primary threats using selected criteria. These primary threats will help the Assessment Team and stakeholders complete the risk assessment and focus on proper mitigation measures.

Selecting Primary Threats

Unlike natural disasters, terrorists continually evaluate, plan, and seek to exploit the weakest building protective design features. Therefore, it becomes impossible both from a technical and benefit/cost point to try to protect everything from every type of attack. The building stakeholders have to make a determination as to what the design basis threat is for their building and what level of protection they can afford. As the terrorist threat changes over time, the building stakeholders may wish to revisit this part of the risk assessment process.

To select your primary threats, the criteria described below have been provided. The selected criteria are part of Table 1-4, which is designed to help you to determine your potential threat. Scores from 1 to 10 (10 being the greater threat) are described.

- **Access to Agent.** The ease by which the source material can be acquired to carry out the attack. Consideration includes the local materials of HazMat inventory, farm and mining supplies, major chemical or manufacturing plants, university and commercial laboratories, and transportation centers.

- **Knowledge/Expertise.** The general level of skill and training that combines the ability to create the weapon (or arm an agent) and the

technical knowledge of the systems to be attacked (heating, ventilation, and air conditioning [HVAC], nuclear, etc.). Knowledge and expertise can be gained by surveillance, open source research, specialized training, or years of practice in industry.

- **History of Threats (Building Functions/Tenants).** What has the potential threat element done in the past, how many times, and was the threat local, regional, national, or international in nature? When was the most recent incident and where, and against what target? Are the building functions and tenants attractive targets for the terrorist?

- **Asset Visibility/Symbolic.** The economic, cultural, and symbolic importance of the building to society that may be exploited by the terrorist seeking monetary or political gain through their actions.

- **Asset Accessibility.** The ability of the terrorist to become well-positioned to carry out an attack at the critical location against the intended target. The critical location is a function of the site, the building layout, and the security measures in place.

- **Site Population/Capacity.** The population demographics of the building and surrounding area.

- **Collateral Damage/Distance to the Building.** The potential of the threat to cause collateral damage or disruption to the building of interest. The building of interest is not considered the primary target.

Table 1-4 is used in conjunction with Table 1-3 to create a general Threat Scenario for the site or building. Table 1-5 illustrates the use of the threat scoring matrix for a typical multi-story commercial office building in an urban area with underground parking, internet enabled environmental energy management system, Voice over Internet Protocol (VoIP) telecommunications system, Internal Protocol/Transmission Control Protocol (IP/TCP) enabled security system using local area network (LAN) and wireless connectivity for closed-circuit televisions (CCTVs) and entry access control, and standard hard wire connectivity for the fire alarm system. Your potential threats will be selected from those reaching the highest scores.

Table 1-4: Criteria to Select Primary Threats

Criteria							
Scenario	**Access to Agent**	**Knowledge/ Expertise**	**History of Threats (Building Functions/ Tenants)**	**Asset Visibility/ Symbolic**	**Asset Accessibility**	**Site Population/ Capacity**	**Collateral Damage/ Distance to Building**
9-10	Readily available	Basic knowledge/open source	Local incident, occurred recently, caused great damage; building functions and tenants were primary targets	Existence widely known/iconic	Open access, unrestricted parking	> 5,000	Within 1,000-foot radius
6-8	Easy to produce	Bachelor's degree or technical school/ open scientific or technical literature	Regional/State incident, occurred a few years ago, caused substantial damage; building functions and tenants were one of the primary targets	Existence locally known/ landmark	Open access, restricted parking	1,001-5,000	Within 1-mile radius
3-5	Difficult to produce or acquire	Advanced training/rare scientific or declassified literature	National incident, occurred some time in the past, caused important damage; building functions and tenants were one of the primary targets	Existence published/ well-known	Controlled access, protected entry	251-1,000	Within 2-mile radius
1-2	Very difficult to produce or acquire	Advanced degree or training/ classified information	International incident, occurred many years ago, caused localized damage; building functions and tenants were not the primary targets	Existence not well-known/ no symbolic importance	Remote location, secure perimeter, armed guards, tightly controlled access	1-250	Within 10-mile radius

Table 1-5: Nominal Example to Select Primary Threats for a Specific Urban Multi-story Building

Criteria									Score
Scenario		**Access to Agent**	**Knowledge/ Expertise**	**History of Threats (Building Functions/ Tenants)**	**Asset Visibility/ Symbolic**	**Asset Accessibility**	**Site Population/ Capacity**	**Collateral Damage/ Distance to Building**	
Improvised Explosive Device (Bomb)									
1-lb. Mail Bomb		9	9	3	8	3	10	1	43
5-lb. Pipe Bomb		9	9	3	8	3	10	2	44
50-lb. Satchel Bomb/Suicide Bomber		8	8	6	8	3	10	3	46
500-lb. Car Bomb		6	8	7	8	3	10	3	45
5,000-lb. Truck Bomb		4	8	5	8	3	10	3	41
20,000-lb. Truck Bomb		2	6	1	8	3	10	3	33
Natural Gas		2	8	1	8	3	10	5	37
Bomb/Aircraft/Ship									
Small Aircraft		9	6	3	8	3	10	3	42
Medium Aircraft		5	4	7	8	3	10	3	40
Large Aircraft		2	3	7	8	3	10	3	36
Ship		0	0	0	8	3	10	3	24
Chemical Agent									
Choking	Chlorine	5	7	2	8	3	10	2	37
	Phosgene	3	10	2	8	3	10	1	37
Blood	Hydrogen Cyanide	3	8	2	8	3	10	1	35
Blister	Lewisite	3	6	2	8	3	10	1	33
Nerve	Sarin	3	4	6	8	3	10	4	38

Table 1-5: Nominal Example to Select Primary Threats for a Specific Urban Multi-story Building (continued)

Scenario		Criteria: Access to Agent	Knowledge/ Expertise	History of Threats (Building Functions/ Tenants)	Asset Visibility/ Symbolic	Asset Accessibility	Site Population/ Capacity	Collateral Damage/ Distance to Building	Score
Biological Agent									
Bacteria	Anthrax	4	5	9	8	3	10	2	41
	Plague	4	5	3	8	3	10	2	35
	Tularemia	4	5	2	8	3	10	2	34
Viruses	Hemorrehagic Fevers	4	5	2	8	3	10	2	34
	Smallpox	2	5	2	8	3	10	2	32
Toxins	Botulinum	5	5	5	8	3	10	2	38
	Ricin	8	8	9	8	3	10	2	48
Radiological Agent									
"Dirty Bomb"		5	7	1	8	3	10	5	39
Spent Fuel Storage		2	6	1	8	3	10	1	31
Nuclear Plant		1	6	1	8	3	10	1	30
Armed Attack									
RPG/LAW/Mortar		4	5	2	8	3	10	2	34
Ballistic		10	10	5	8	3	10	2	48
Cyber Attack									
Worm		9	10	5	8	3	10	1	46
Virus		9	10	5	8	3	10	1	46
Denial of Service		9	7	5	8	3	10	1	43

Note that the values for "Asset Visibility/Symbolic," "Asset Accessibility," and "Site Population/Capacity" are constants because a single building is being analyzed.

For the nominal example, the five primary threats that will be examined include:

- **Vehicle Bomb.** 500-lb. car bomb detonating within 15 feet of building exterior
- **Chemical Agent.** Sarin gas most toxic of the listed agents; assumed worst case
- **Biological Agent.** Recent mail attacks with Ricin; no antidote, high economic productivity loss
- **Cyber Attack.** Impact on Emergency Management Systems (EMS), VoIP telecommunications, security systems

The "dirty bomb" and armed assault are other potential threats that could be considered, but are left out of this analysis for simplicity.

These examples reveal subjective estimates and summed scores and provide a first level analysis of the primary threats that may affect your site or building. To complete this portion of your risk assessment, you should use Worksheet 1-1.

Determining the Threat Rating (Task 1.4)

Having selected the primary threats for your site or building, the next step is to determine how the threat will affect the functions and critical infrastructure. The threat rating is an integral part of the risk assessment and is used to determine, characterize, and quantify a loss caused by an aggressor using a weapon or agent and tactic against the target (asset). The threat rating deals with the likelihood or probability of the threat occurring and the consequences of its occurrence.

For determining the threat rating, this How-To Guide provides a methodology based on consensus opinion of the building stakeholders, threat specialists, and engineers. (This group could be expanded as necessary to help refine the scoring process.) Table 1-6 provides a scale to help you with this process. The scale is a combination of a 7-level linguistic scale and a 10-point numerical scale (10 being the greater threat). The key elements of this scale are the likelihood/credibility of a threat, potential weapons to be used during a terrorist attack, and information available to decision-makers. The primary objective is to look at the threat, the geographic distribution of functions and critical infrastructure, redundancy, and response and recovery to

evaluate the impact on the organization should a primary threat attack occur. Tables 1-7A and 1-7B display a nominal example of applying these ratings for an urban multi-story building.

Table 1-6: Threat Rating

Threat Rating		
Very High	10	Very High – The likelihood of a threat, weapon, and tactic being used against the site or building is imminent. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is credible.
High	8-9	High – The likelihood of a threat, weapon, and tactic being used against the site or building is expected. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is credible.
Medium High	7	Medium High – The likelihood of a threat, weapon, and tactic being used against the site or building is probable. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is credible.
Medium	5-6	Medium – The likelihood of a threat, weapon, and tactic being used against the site or building is possible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is known, but is not verified.
Medium Low	4	Medium Low – The likelihood of a threat, weapon, and tactic being used in the region is probable. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is known, but is not likely.
Low	2-3	Low – The likelihood of a threat, weapon, and tactic being used in the region is possible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat exists, but is not likely.
Very Low	1	Very Low – The likelihood of a threat, weapon, and tactic being used in the region or against the site or building is very negligible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is non-existent or extremely unlikely.

Worksheet 1-2 helps you organize and determine the threat rating in terms of building functions and infrastructure (see Task 2.3). The purpose is to produce a more informed opinion regarding the manmade hazards that affect your assets.

As a starting point, use a value of 5 and assume a medium level of threat; then adjust the threat rating up or down based on consensus. Note that the threat rating is independent of the building function and infrastructure because it is assumed to be ubiquitous to the entire building and the same threat numeric value is used vertically for each function or infrastructure component (see Tables 1-7A and 1-7B).

Table 1-7A: Nominal Example of Threat Rating for an Urban Multi-story Building (Building Function)

Function	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Administration	8	4	5	2	2
Engineering	8	4	5	2	2
Warehousing	8	4	5	2	2
Data Center	8	4	5	2	2
Food Service	8	4	5	2	2
Security	8	4	5	2	2
Housekeeping	8	4	5	2	2
Day Care	8	4	5	2	2

Table 1-7B: Nominal Example of Threat Rating for an Urban Multi-story Building (Building Infrastructure)

Infrastructure	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Site	8	4	5	2	2
Architectural	8	4	5	2	2
Structural Systems	8	4	5	2	2
Envelope Systems	8	4	5	2	2
Utility Systems	8	4	5	2	2
Mechanical Systems	8	4	5	2	2
Plumbing and Gas Systems	8	4	5	2	2
Electrical Systems	8	4	5	2	2
Fire Alarm Systems	8	4	5	2	2
IT/Communications Systems	8	4	5	2	2

WORKSHEET 1-1: SELECTION OF PRIMARY THREATS

Worksheet 1-1 will help you to select your primary threats. Building stakeholders and the Assessment Team should review criteria provided in Task 1.3 of this How-To Guide to fill out this Worksheet. After ranking each threat against the provided criteria (Table 1-2), the threat scores should be summed. The top scoring threats (select three to ten of the threats based on score dispersion) become the major threats that you will use for the preparation of your risk assessment.

Criteria								Score
Scenario	**Access to Agent**	**Knowlege/ Expertise**	**History of Threats (Building Functions/ Tenants)**	**Asset Visibility/ Symbolic**	**Asset Accessibility**	**Site Population/ Capacity**	**Collateral Damage/ Distance to Building**	
Improvised Explosive Device (Bomb)								
1-lb. Mail Bomb								
5-lb. Pipe Bomb								
50-lb. Satchel Bomb/ Suicide Bomber								
500-lb. Car Bomb								
5,000-lb. Truck Bomb								
20,000-lb. Truck Bomb								
Natural Gas								

WORKSHEET 1-1: SELECTION OF PRIMARY THREATS (CONTINUED)

Scenario		Criteria: Access to Agent	Knowlege/ Expertise	History of Threats (Building Functions/ Tenants)	Asset Visibility/ Symbolic	Asset Accessibility	Site Population/ Capacity	Collateral Damage/ Distance to Building	Score
Bomb/Aircraft/Ship									
Small Aircraft									
Medium Aircraft									
Large Aircraft									
Ship									
Chemical Agent									
Choking	Chlorine								
	Phosgene								
Blood	Hydrogen Cyanide								
Blister	Lewisite								
Nerve	Sarin								
Biological Agent									
Bacteria	Anthrax								
	Plague								
	Tularemia								
Viruses	Hemorrehagic Fevers								
	Smallpox								
Toxins	Botulinum								
	Ricin								

WORKSHEET 1-1: SELECTION OF PRIMARY THREATS (CONTINUED)

Criteria								Score
Scenario	**Access to Agent**	**Knowlege/ Expertise**	**History of Threats (Building Functions/ Tenants)**	**Asset Visibility/ Symbolic**	**Asset Accessibility**	**Site Population/ Capacity**	**Collateral Damage/ Distance to Building**	
Radiological Agent								
"Dirty Bomb"								
Spent Fuel Storage								
Nuclear Plant								
Armed Attack								
RPG/LAW/Mortar								
Ballistic								
Cyber Attack								
Worm								
Virus								
Denial of Service								

WORKSHEET 1-2: THREAT RATING

Function	Threat Rating (one column for each threat)	Infrastructure	Threat Rating (one column for each threat)
Administration		Site	
Engineering		Architectural	
Warehousing		Structural Systems	
Data Center		Envelope Systems	
Food Service		Utility Systems	
Security		Mechanical Systems	
Housekeeping		Plumbing and Gas Systems	
Day Care		Electrical Systems	
Other		Fire Alarm Systems	
Other		IT/Communications Systems	

Worksheet 1-2 can be used to complete your risk assessment and will be used in conjunction with Worksheets 4-1 and 4-2. It can be used to discuss priority threats with building stakeholders and among the members of the Assessment Team. To fill out this table, analyze the impact of a particular threat on the building core functions and building infrastructure components of your building. Use the results of Worksheet 1-1 to assist you in this process. Building core functions and building infrastructure components are defined in Section 2.3 of this How-To Guide.

Threat Rating	
Very High	10
High	8-9
Medium High	7
Medium	5-6
Medium Low	4
Low	2-3
Very Low	1