Terrorism

Assessing the risk of WMD & minimizing exposure

By Brian T. Bennett

SINCE SEPT. 11, 2001, the U.S. has been under the increased threat that terrorists may attempt additional attacks. Threats come in different forms and from different sources. Threats from outside a facility could affect people and the facility itself, and may involve trespassing, unauthorized entry, theft, burglary or vandalism. Threats from inside the facility may arise due to inadequate designs, management systems, staffing or training, or other internal problems. These may include theft, substance abuse, sabotage, disgruntled employee or contractor actions, or workplace violence.

Threats are not restricted to people and property; they could also involve sensitive facility information. Facility outsiders, employees or contractors could pose threats to data storage and transmissions of, for example, proprietary information, privacy data and contract information. They could also pose a threat to computer-controlled equipment. Such threats may include breaches in data access and storage, uncontrolled dissemination or destruction of information, or threats to automated information systems (EPA). Potential terrorist targets include national landmarks, critical infrastructure such as bridges, tunnels and power plants, areas with high population, and commercial and industrial facilities. This article offers guidelines for assessing the risk posed by terrorists, their potential use of weapons of mass destruction (WMD), and what can be done to protect facilities and employees.

What Is Terrorism?

Terrorism is defined as the "premeditated, politically motivated violence perpetrated against non-combatant targets by subnational groups or clandestine agents usually intended to influence an audience" [USC Title 22, Sec. 2656f(d)]. Simply translated, this means groups that perform criminal acts which are meant to instill fear, coerce or intimidate people in order to get them to alter their beliefs and/or day-to-day activities. The basic goals of terrorism are to cause casualties, destroy critical infrastructure, disrupt the economy and interrupt daily routine.

The threat of terrorism is dynamic and has evolved in response to social, political and technological changes. It has been around for centuries (sidebar, pg. 32), and it's not new in the U.S. (Figure 1). The very nature of terrorism is what is most disturbing. These acts are unanticipated, premeditated, intimidating, politically motivated and display a complete disregard for human life. Terrorism impacts the general public in two ways: 1) it instills fear by its ability to strike directly against personal security; 2) it is random and will impact whomever happens to be in the wrong place at the wrong time. Terrorism takes on many forms, including kidnapping, assassination, cyber attacks and the use of WMD.

Weapons of Mass Destruction

Use of WMD is a type of terrorism that would most easily cause widespread casualties, destroy property and cause economic damage. The sidebar on pg. 34 lists recent incidents involving WMD. To understand how to detect and prevent these incidents, the threat must be understood. WMD come in five basic forms: biological, nuclear, incendiary, chemical and explosive (widely known by the acronym "B-NICE").

Biological

Biological warfare agents are the most feared by emergency responders and public health officials. Biological weapons consist of bacteria (such as anthrax, plague and Q-fever) that are single-celled free living organisms which reproduce by simple division and are easy to grow; viruses (such as smallpox and ebola), which are organisms that are smaller than bacteria and require living cells in which to reproduce and are intimately dependent on the body they infect; and toxins (such as ricin and botulism), which are poisons made from naturally occurring materials.

Biological weapons are insidious in that they can be disseminated, thereby exposing large numbers of people without any apparent immediate indication. Those exposed can then spread the agent as they travel. The first indication that a biological attack has occurred would be when people start to become symptomatic and present themselves at medical facilities for treatment.

Nuclear

The chance of a major nuclear detonation occurring within the U.S. is considered remote. However, radiological contamination

Brian T. Bennett, Ph.D., CSP, CHMM, *is a safety manager for Akzo Nobel Polymer Chemicals LLC in Edison, NJ, where he has been employed for 16 years. Bennett holds a B.S. in Chemical Engineering, an M.S. in Occupational Safety and a Ph.D. in Safety Engineering. He is a professional member of ASSE's New Jersey Chapter and is a member of the New Jersey Governor's Terrorism Task Force.*

18th-20th Century Examples of Terrorism

- Russians catapult plague infected corpses into areas held by Sweden.
- Religious violence against Catholics, Quakers and others by Puritans in American colonies.
- Anti-government tax protester violence after the revolutionary war in America.
- British officials provide blankets from smallpox patients to Native Americans.
- 12 office holders assassinated following the killing of President Lincoln.
- KKK violence starts.
- Haymarket Square bombing in Chicago.
- Catholic churches burned in Boston and Philadelphia.
- IWW activists blow up Bunker Hill and Sullivan mines in Wadner, ID.
- 1950 assassination attempt on President Truman.
- 1954 shooting in U.S. House of Representatives.
- 1972 Frances Tavern bombing.
- 1975 LaGuardia Airport bombing.
- 1981 Kennedy Airport bombing.
- 1983 U.S. Senate bombing.
- 1993 World Trade Center (WTC) bombing.
- 1995 Amtrak derailment, Arizona.
- 1995 Freeman Group salmonella attack, Oregon.
- 1995 Oklahoma City bombing.
- 2001 WTC and Pentagon attacks.

through the use of a smaller "dirty bomb" or ''suitcase" device, or through the deliberate release of radiation, is considered more likely. Dirty bombs (otherwise known as radiological dispersion devices) consist of radioactive material that is packed around conventional explosives and spread through the detonation of those explosives. Although not conventional nuclear weapons, these devices can effectively spread radiation in relatively small areas. A suitcase device is a small-order nuclear weapon contained in a small package.

Radiation can also be spread over large areas by deliberate release. Possible sources of radioactive material that can be released exposing relatively large populations may include an attack on a nuclear facility, hijacking shipments of radioactive materials or theft from secure facilities.

Incendiary

Incendiary attacks use fire as a weapon to destroy property and cause injury or death. Incendiary devices are ignited with 75-percent reliability; less than five percent of these incidents are preceded by a threat (USFA/FEMA).

Chemical

Chemical agents most commonly cause damage by either inhalation of the agent, or by skin exposure that leads to acute localized effects or systemic effects caused by absorption. Chemical agents typically fall into one of five classes:

1) **Nerve agents.** These materials act on all parts of the nervous system and are similar to pesticides in function. Examples include sarin and V agent (VX).

2) **Vesicants.** Also known as blister agents, these chemical agents cause large, painful blisters on any body area exposed, including the skin and respiratory tract. Examples include mustard gas and lewisite.

3) **Blood agents.** These common industrial chemicals can interfere with the blood's ability to absorb and distribute oxygen to the body systems. Cyanide compounds are an example.

4) **Choking agents.** These materials are also common industrial chemicals that can cause eye and airway irritation, difficulty breathing and pulmonary edema (chemical pneumonia). Examples include chlorine and phosgene.

5) **Irritants.** These agents are often used as riot control agents by law enforcement authorities. These materials temporarily incapacitate a victim but cause few long-term effects. Common irritants include tear gas and pepper spray.

Explosive

Bombing has become the "tactic of choice," with 70 percent of all terrorist incidents involving explosives (USFA/FEMA). As noted, explosives can be used to disperse biological, chemical or nuclear agents. Terrorists have become proficient at developing improvised devices to carry explosives, including vehicles, pipes, packages and suicidal individuals.

Protecting People & Facilities

With a basic understanding of WMD and the threats they pose, the protection process can begin. Since it is difficult to predict the next terrorist target and the type of attack, preparation is key. WMD scenarios originate with deliberate acts (rather than equipment or human failures); thus, the safeguards installed to prevent accident scenarios may not be adequate to protect against terrorist threats. Therefore, the purpose of terrorism protection planning should be to "detect, deter, delay and respond."

What Is the Threat?

A company may be the *target.* If the firm is highly visible and involved in a controversial business, the potential for casualties and adverse economic impact may be high. The site may be *collateral damage,* in that a facility may be adversely impacted by an attack on critical infrastructure (e.g., local power plant). In addition, employees could be impacted by a dispersed agent or may be close to the intended target. A facility may be used as a *diversionary attack* in an attempt to draw responders away from the real attack. Or, company materials may be *diverted* (stolen or hijacked) by groups hoping to use the materials to create WMD.

Figure 1

Suspected Terrorist Activities: U.S.

The threat of terrorism affects all communities; history has shown that no community is immune. Terrorism transcends all geographic and demographic boundaries. While not all the incidents cited have been determined to be terrorism, they are all suspicious criminal acts that may be linked to terrorist activity.

Eastern U.S. (east of Mississippi River)

- In February 1993, the World Trade Center was damaged by a vehicle bomb, killing six people.
- In July 1993, a member of the Animal Liberation Front set a fire in a Michigan State University research facility.
- In 1995, a Harrisonburg, VA, neurologist was charged with possession of ricin with intent to use it to kill his former boss.
- In April 1996, members of the Georgia Militia were arrested for plotting to make pipe bombs.
- In September 1996, a Staten Island, NY, man accused of stockpiling weapons was arrested by ATF agents.
- In October 1996, seven men with connections to a local anti-government paramilitary group were arrested on charges of plotting to blow up the Criminal Justice Information Services complex near Clarksburg, WV.
- In 1996, a Romanian immigrant was stopped as he attempted to board a flight in Tampa, FL, carrying five explosive devices, weapons and 180 rounds of ammunition.
- In January 1997, several letter bombs were sent to the offices of the Al Hayat Publishing Co. offices in the National Press Building in Washington, DC.
- In 1996 and 1997, numerous bombing incidents occurred in the Atlanta area including at least two with confirmed secondary devices.
- In September 2001, terrorists hijack four airliners, crashing them into the WTC, Pentagon and a Pennsylvania field.

Central U.S.

- In March 1995, members of the Patriot's Council in central Minnesota were arrested and charged with manufacturing ricin to kill law enforcement officers.
- In April 1995, the Alfred P. Murrah Federal Building in Oklahoma City was bombed; 168 people were killed and hundreds injured.
- In November 1995, charges were filed against an "anti-government prophet" in Muskogee, OK, for plotting a series of bombings against abortion clinics, civil rights offices and government facilities.
- In December 1995, a man charged with possession of ricin in Arkansas killed himself in his jail cell.
- In May 1996, an explosion blew out the windows in a building housing an FBI field office in Laredo, TX.
- In August 1996, a person was sentenced for plotting to bomb the office of the IRS in Austin, TX.
- Also in 1996, a man identified as a member of an anti-government freeman group was apprehended in Topeka, KS, and authorities found a bomb-triggering device in his car.

Western U.S.

- In October 1995, the Amtrak Sunset Limited was derailed by sabotaged tracks near Hyder, AZ. This incident killed one and seriously injured 12.
- In December 1995, there was an attempted bombing of the IRS building in Reno, NV.
- In January 1996, an explosion took place outside of a U.S. Forest Service headquarters in Espanola, NM.
- In April 1996, a bomb exploded in the truck of a federal employee, injuring him and his wife in Vacaville, CA.
- In April 1996, Theodore Kaczynski was arrested as the suspected Unibomber.
- In June 1996, members of the Viper Militia were arrested in Phoenix, AZ, and charged with conspiracy to make bombs and use deadly weapons.
- In June 1996, members of the Washington State Militia and a Seattle-based Freeman group were arrested on federal conspiracy charges.

Source: "Terrorism in the United States."

The threat of terrorism is dynamic and has evolved in response to social, political and technological changes.

Recent WMD Incidents

Apr. 25, 1997: Four members of the True Knights of the Ku Klux Klan plotted to bomb a natural gas refinery in Dallas, releasing a deadly cloud of hydrogen sulfide gas as a diversion for the robbery of an armored car across town. *Source:* <http://www.vpc.org/studies/ducktwo.htm>.

Apr. 23, 2000: An Australian man was found guilty of hacking into the Maroochy Shire, Queensland Australia's computerized waste management system and causing millions of gallons of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel. The district court found that the 49-year-old man had conducted a series of electronic attacks on the sewage control system after a job application he had made was rejected. At the time, he was employed by the company that had installed the system. *Source:* <http://www.theregister.co.uk/content/4/22579.html>.

Sept. 21, 2001: An explosion at an ammonium nitrate plant in Toulouse, France, killed 23 employees and seven persons offsite and injured as many as 10,000. There was extensive damage to hundreds of homes, schools, and businesses. The incident was investigated as a possible terrorist attack. *Source:* <http://www.usatoday.com/news/sept11/2001/10/04/toulouse.htm>.

Oct. 5, 2001: The Trans-Alaska Oil Pipeline was shut down for three days after someone shot a bullet into the pipeline. Crews struggled to plug the hole and clean up the more than 260,000 gallons of oil spilled. *Source:* <http://www.seattletimes.nwsource.com/html/nationworld/134350375_pipeline06m0.htl>.

Apr. 11, 2002: An al Qaeda operative used a fuel truck in a suicide attack against the oldest synagogue in North Africa, located on the island of Djerba in Tunisia. The attack killed 21 people. *Source:* <http://www.cnn.com/2002/WORLD/africa/04/12/tunisia.toll>.

May 22, 2002: A remote-controlled bomb exploded in a tank truck as it was being filled with diesel fuel at Israel's largest fuel depot in Tel Aviv. *Source:* <http://www.newstribune.com/stories/052302/wor_0523020934.asp>.

Oct. 6, 2002: A small boat crashed into a French oil tanker carrying 400,000 gallons of crude oil and exploded off the coast of Yemen. *Source:* <http://www.abc.net.au/am/s694714.htm>.

Oct. 14, 2002: al Qaeda bombed a nightclub in Bali, Indonesia killing more than 180 and injuring hundreds. *Source:* http://www.cnn.com/2002/WORLD/asiapcf/southeast/10/14/bali.alqaeda>.

Nov. 28, 2002: Suicide bombers killed 12 people at an Israeli-owned beach resort in Kenya, and fired two missiles which narrowly missed an airliner that just took off from the airport in Mombasa. *Source:* <http://www.abc.net.au/news/2002/11/item20021128181616_1.htm>.

May 11, 2003: A bomb exploded in a crowded market in Koronadel, Philippines, killing nine and wounding 41. The blast is blamed on the Muslim separatist Moro Islamic Liberation Front. *Source:* <http://www.manilatimes.net>.

May 12, 2003: Four explosions rocked Riyadh in an attack on compounds housing Americans, other westerners and Saudis, killing 34. Officials have linked suspects in the attack to al Qaeda. *Source:* The Star Ledger, *Newark, NJ, May 19, 2003.*

May 16, 2003: Bomb attacks in Morocco killed 28 people and injured more than 100. The government blames "international terrorism," and investigates local militants linked to al Qaeda. *Source:* The Star Ledger, *Newark, NJ, May 19, 2003.*

Where to Start?

The protection process involves three broad steps: identify potential targets; quantify the risk an attack may pose; and suggest appropriate countermeasures to reduce risk. The protection process consists of a four-part plan:

1) Assess the risk: What are the vulnerabilities present at a given facility?

2) Evaluate the risk: What is the possibility of an attack involving employees or impacting a given facility?

3) Reduce the risk: How can the facility's vulnerabilities be minimized?

4) Re-evaluate the risk: How can the plan be improved?

Facilities cannot prevent or protect against all known or suspected threats. However, some reasonable measures and approaches can be taken for certain threats. Remember, threat = capability + intent + motivation + ease.

Assessment Team

A team should be assembled to assess the risks; it should include representatives from operations, maintenance, technical/engineering, transportation, safety and health, and environmental. Hourly employees should also be included in order to encourage employee involvement and ownership. In addition, these employees may be aware of security issues that management has not yet identified.

Assess the Risk

Risk assessment is defined as a comprehensive review of the facility, its products or services, and its people to determine risk vulnerabilities. Vulnerabilities can be defined as what is present on the site, what product is made or provided, and what about a facility's location makes it an attractive target. The risk assessment process consists of three stages: risk characterization, risk screening and risk assessment.

Risk Characterization

Risk characterization asks two basic questions: What does this site have that could be used as a WMD? Could this site be the target of a WMD attack? An affirmative answer to either question leads to the next step.

Risk Screening

The formal assessment process starts with a screening process that examines a facility's "critical assets"—which include utilities, critical equipment, manufacturing buildings, all storage tanks, maintenance areas, warehouses, computer systems and large groups of people. Each asset would be evaluated to determine the consequences of a successful attack against five criteria: casualties, environmental impact, economic impact, business impact and impact on the facility's infrastructure. Figure 2 offers an example of a facility screening assessment methodology. Once each critical asset and scenario has been screened, scores are used to set priorities for conducting a complete vulnerability assessment. The sidebar on pg. 36 presents an example of a completed facility scenario screening.

Several questions must be answered during the screening phase. These include:

- What does this site have: Large groups of people? Explosive, nuclear, biological or chemical materials?
- What does the facility make or provide: Explosive, nuclear, biological or chemical materials? Controversial services? Essential services (e.g., water treatment facility)?
- Where is the site located: Shares an occupancy with a potential target (e.g., governmental agency)? In or near a high-profile structure that holds historic, religious or national importance? In heavily populated areas? In gridlocked areas with limited access/egress?

Risk Assessment

The risk assessment process—also called security vulnerability analysis—must be comprehensive, much more detailed than the risk screening and must cover all aspects of the operation. The ability to consider all vulnerabilities is critical. One great challenge the assessment team will face is the fact that risk has traditionally been assessed using scenarios that originate with traditional equipment or human failures. Now, the team must consider scenarios that originate with an intentional act—against which traditional accident or hazard safeguards may not be sufficient.

The risk assessment generally focuses on current activities and practices.

- What are the facility and its employees doing now?

Figure 2

Facility Screening Assessment

Casualties
0 None expected
1 Site and/or offsite non-life-threatening injuries likely
2 Site and/or offsite life-threatening injuries likely
3 On-site fatalities likely
4 Off-site fatalities likely

Environmental
0 Biodegradable
1 Will not leave the facility site
2 Likely to leave the site; however, nonpersistent and no decontamination required
3 Likely to leave the site; however, nonpersistent and decontamination required
4 Likely to leave the site; persistent and long-term remediation required

Economic
0 No significant effect likely
1 Impact on the facility's profitability >10 percent
2 Impact corporation's profitability >10 percent
3 Impact U.S. economy
4 Impact world economy

Business Interruption
0 Startup facility with minor modifications
1 Facility shutdown < 1 month
2 Facility shutdown < 6 months
3 Facility shutdown < 1 year
4 Facility not expected to be rebuilt

Infrastructure
0 No effect on operations
1 Damage limited to the specific building/area only
2 Damage to support systems and/or utilities
3 Damage to other production units
4 Damage to the entire site

Weighting Factors

Casualties	Rating x 5
Environmental	Rating x 4
Economic	Rating x 3
Business Interruption	Rating x 2
Infrastructure	Rating x 1

Scoring

Maximum possible score = 60

Score of	Must be addressed in
41-60	1 year
21-40	2 years
1-20	3 years

Additionally:
- Any individual rating of "4" must be corrected within one year.
- Any individual rating of "3" must be corrected within two years.

Sample Risk Screening

Scenario: Poisonous phosgene gas is admitted into the HVAC system of a local mall.

Explanation of results

Casualties: 3 x 5 = 15. Gas contained to building; no one offsite would be impacted.

Environmental: 2 x 4 = 8. Gas likely to leave the building, but in low concentrations.

Economic: 1 x 3 = 3. Business would be shut down for a period of time for the investigation; some people would be scared and not shop at the mall in the future.

Business Interruption: 1 x 2 = 2. The mall would likely be closed less than one month for the investigation, etc.

Infrastructure: 1 x 1 = 1. Consequences would only effect the mall itself, as it did not supply infrastructure services to other facilities.

Total: 29

Conclusions

Specific countermeasures must be implemented within two years to reduce the risk of on-site fatalities (due to the Casualties rating of 3).

Countermeasures to reduce the risk for the entire mall should be implemented within two years (due to total score of 29).

- What could go wrong?
- Are there any special areas of concern?
- What could be done differently?

The assessment must also encompass a review of critical infrastructures and how an attack on them might affect the site. These infrastructures include electric power, natural gas, water, communications, highways, bridges and tunnels, and raw material suppliers. The goal is to fully understand the current situation, identify possible vulnerabilities and develop a plan to minimize damage to employees and assets, as well as to the community and the environment.

The risk assessment process should be asset- and scenario-based. Asset-based assessments evaluate the impact a successful attack would have on a particular target. Scenario-based assessments evaluate a particular situation (or attack) that may be used against the asset. For example, the asset (target) may be a high-rise office building and the scenario (attack) may involve the use of poisonous gas admitted into the HVAC system.

Evaluating the Risk

Once risk has been assessed, it must be evaluated and priorities determined. Each vulnerability addressed during the assessment process should be scrutinized for its WMD potential. Each scenario should be evaluated to determine the potential difficulty and severity of attack, as well as the attractiveness of a successful attack. Terrorism is not always designed solely to cause casualties; an attack may be carried out to harm the economy, destroy a business, or cause corporate and personal financial losses. Several risk evaluation tools are available; they often include a system for assigning a numeric value to rank risks. Typical factors evaluated to assign the risk factor include the effect on:

- company personnel;
- public health (in terms of casualties);
- public welfare (in terms of being unable to provide an essential product or service);
- the environment;
- the company's finances;
- the company's operational sustainability;
- the national or international economy;

Reducing the Risk

At this point, a plan to eliminate (or minimize) each vulnerability and reduce both the risk of a successful attack and the unfavorable outcomes of such an attack should be developed. One effective way to reduce risk is to incorporate inherent safety into all operations. The hierarchy of inherent safety includes:

1) Reduce or eliminate the possibility of an attack by using inherently safe materials and technologies.

2) Reduce the probability of negative impacts through secondary prevention measures.

3) Reduce potential severity of the impacts by coordinating response with local authorities and developing plans for appropriate mitigation measures.

When selecting countermeasures to reduce risk, the team must determine whether current security measures effectively address these new threats.

Reevaluating the Risk

The overall assessment process should include a provision that mandates periodic re-evaluation of security programs. This process can serve as a validation that changes made have been effective; it also serves to identify previously undiscovered vulnerabilities. The re-evaluation should be conducted by a person(s) who was not involved in the original assessment in order to have an unbiased, "fresh" look at the facility. A law enforcement representative or reputable security specialist should participate in the validation of the overall security program. Involving local law enforcement in this process meets the requirement for community involvement, and also helps to ensure that the faculty's written plans are coordinated with those of the municipality.

Potential Security Enhancements

Some best practices include:

1) **Communicate with authorities.** The crucial step in the risk reduction phase is coordination with local, state and federal law enforcement and emergency response agencies. The facility's risk reduction plans must be incorporated into the local emergency response plan. These agencies are a valuable resource and can provide effective risk reduction techniques. Additionally, these agencies must be fully informed so they can provide appropriate emergency response in the event of an attack.

2) **Ensure physical security/perimeter protection/access control.** Increased hardening may be needed to restrict access to a facility. Increased physical security and perimeter protection includes fencing, concrete barriers, surveillance cameras, increased security patrols, defoliation of fencelines to increase

observation and intrusion detection systems. All facility entrances should be locked and, preferably, guarded. Employees should be required to use an access control system (swipe card or password-protected electronic locks) to enter. Adequate lighting should be provided to facilitate perimeter surveillance. Projectile shields can be used to protect vulnerable targets. Landscaping should be installed to block clear lines of sight of key infrastructures from the public way.

3) **Install a backup system for utilities.** A backup should be in place for any critical infrastructure that could lead to an emergency or increase its severity. If this is not possible, efforts should be made to reduce the negative effect of their loss should an attack occur.

4) **Conduct training and implement relevant plans, policies and procedures.** Written plans must be developed to address the specific response to identified vulnerabilities. For example, many sites have a program through which designated employees screen incoming mail for suspicious packages; these employees are specially trained to identify and handle such packages. Other written policies and procedures, along with the associated awareness training, that should be implemented may include:

- access control;
- background checks for employees, contractors and truck drivers;
- dealing with civil disturbances;
- employee misconduct policy;
- general weapons policy;
- identification, handling and reporting of suspicious people, activities, inquiries or calls;
- personnel and vehicle search procedures;
- protection of electronic and proprietary information procedure;
- workplace violence policy.

5) **Perform background checks of new employees and contractors.** Background checks help ensure that potential employees or contractor personnel have no history that is of concern. Various types of background checks are available; useful checks include:

- criminal background check;
- national felony conviction check;
- felony conviction check for each county of residency or employment;
- check FBI's terrorist "be on the lookout" list;
- credit check, which helps to establish the history of residency, employment and sources of income;
- citizenship/immigration check to determine whether the individual is a U.S. citizen, is in the country legally and is authorized to hold a job.

If a company does not want to take responsibility for conducting background checks of contractors, it should require that contractor management certify, in writing, that these checks were completed as specified and were found to be acceptable.

6) **Conduct background checks for truck drivers.** Such checks should be completed for drivers who transport dangerous or sensitive materials into or out of a facility. This check should include the same elements as those for employees and contractors.

7) **Report security incidents.** A procedure that outlines how workers can report security-related incidents to management should be established. All such incidents should be thoroughly investigated so corrective actions can be implemented.

8) **Protect a facility's HVAC system.** Facilities that have large populations in a single building are a potentially attractive target due to the high concentration of people in a relatively small area. HVAC system air intakes are a potential introduction source

Homeland Security Advisory System

The federal government has developed the Homeland Security Advisory System (HSAS), a standardized threat warning system to publicize the current terrorist threat level. The system was intended to create a common vocabulary and a common understanding of the meaning behind the changes in threat conditions (FBI). Threat conditions can be assigned nationally, regionally, by infrastructure sector or to a potential target. Factors considered when assigning these levels include:

- To what degree is the threat information credible?
- To what degree is the threat information corroborated?
- To what degree is the threat specific and/or imminent?
- How grave are the potential consequences of the threat?

HSAS uses a five-tier, color-coded system to indicate the current threat level. Facilities should implement a corresponding set of protective measures to further reduce vulnerability or increase response capability during a period of heightened alert (Bush).

Low Condition (Green): Low risk of terrorist attack.

- Refine and exercise protective measures.
- Train personnel on specific measures.
- Regularly assess facilities for vulnerabilities and take corrective action as needed.

Guarded Condition (Blue): General risk of terrorist attack.

- Check communication systems.
- Review/update emergency response procedures.
- Provide the public with necessary information.

Elevated Condition (Yellow): Significant risk of terrorist attack.

- Increase surveillance of critical locations.
- Coordinate emergency plans with local jurisdiction.
- Assess further refinement of protective measures.
- Implement emergency and contingency plans.

High Condition (Orange): High risk of terrorist attack.

- Coordinate security efforts with armed forces or law enforcement.
- Take additional precautions at public events.
- Prepare to work at an alternate site with a dispersed workforce.
- Restrict access to essential personnel.

Severe Condition (Red): Severe risk of terrorist attack.

- Assign emergency response personnel and pre-position equipment.
- Monitor, redirect or constrain transportation systems.
- Close public and government facilities.
- Increase or redirect personnel to address critical emergency needs.

Employees must know how to detect, deter and respond to possible terrorist activity in order to protect themselves.

for chemical, biological or radiological weapons. Therefore, the system's design and operation must be thoroughly assessed. In particular, air intakes, which are usually easily accessible, must be protected:

- Restrict access to intakes by providing locked fencing around the facility.
- Restrict access to rooftop units via locked doors or access ladders.
- Duct intakes as high as possible to restrict direct access.
- Grate and slope intakes to make it difficult to throw something inside them.
- Monitor intakes with intrusion alarms, cameras and frequent patrols.

9) **Prepare for emergency response.** As noted, facilities must develop comprehensive written emergency response plans and coordinate those plans with local responders. Periodic mock drills should be conducted to test the plans and identify needed updates. Facility evacuation and personnel accountability procedures are especially critical in an emergency, and these procedures should be practiced regularly by all employees.

If the overall assessment process indicates that a facility is a potential target or may be impacted by a nearby potential target, the company may wish to develop some level of internal emergency response capability. This would require training and equipment necessary to provide at least a basic capability for facility personnel to don appropriate PPE, rescue and treat victims, conduct air monitoring for chemical and radiological agents, and decontaminate personnel and victims.

Dealing with the Community

As noted, a clear communications and information link must be maintained with local authorities. Any security-related information should be cleared with law enforcement officials before it is released to the general public or media. Security discussions with the community should be limited to generalities. In addition, any information that could be used to facilitate an attack should be removed from brochures and websites. Other considerations for dealing with the community:

- Restrict participation in security assessments to company and/or law enforcement authorities.
- Do not share findings from site security assessments with the media or general public.
- Reconsider providing facility tours or hosting open houses.
- Redirect requests for right-to-know information or MSDS from unknown people to local authorities.

Conclusion

Everyone must know how to recognize potential terrorist activity or threats and the importance of how they should respond. People must maintain constant vigilance to ensure that facilities are secure and would discourage a possible attack. Even though a facility may not be the specific target, it may be adversely impacted should a nearby target be attacked. Emergency response assistance from local, state or federal authorities may be hours or even days away, depending on the severity and type of attack. Employees must know how to detect, deter and respond to possible terrorist activity in order to protect themselves. Emergency response plans must be coordinated and practiced with local authorities. All employees should be trained on awareness and response issues. "The fact that we are arguably the world's most powerful nation does not bestow invulnerability; in fact, it may make us a larger target for those who don't share our interests, values or beliefs. . . . We must take care to be on guard watching our every step and looking far ahead" (Tenet). ■

References

"Bomb Targets Israeli Main Fuel Depot." Jefferson City News Tribune Online Edition. May 23, 2002. <http://www.newstribune.com/stories/052302/wor_0523020934.asp>.

Brissenden, M. "Small Boat May Have Caused Oil Tanker Explosion." As reported on AM in Australia. <http://www.abc.net.au/am/s694714.htm>.

Bush, G.W. "Homeland Security Advisory System." Homeland Security Presidential Directive—3. Washington, DC: The White House, March 11, 2002.

Centers for Disease Control and Prevention (CDC). "Guidelines for Health Departments." Atlanta: CDC, Oct. 14, 2001.

Environmental Protection Agency (EPA). "Chemical Accident Prevention: Site Security." Washington, DC: EPA, Feb. 2000.

Federal Bureau of Investigations (FBI). "Terrorism in the United States, 1995." FBI and Security Awareness Bulletin 3-96. Washington, DC: U.S. Dept. of Justice, FBI, 1996.

Fischer, L. "Looking for the Unexpected." Security Awareness Bulletin 3-96. Richmond, VA: DoD Security Institute, 1996.

New Jersey State Police. "Weapons of Mass Destruction Technician." West Trenton, NJ: NJ State Police.

NIOSH. "Guidance for Protection of Building Environments from Airborne Chemical, Biological or Radiological Attacks." Washington, DC: Dept. of Health and Human Services, CDC, NIOSH, May 2002.

Smith, T. "Hacker Jailed for Revenge Sewage Attacks." *The Register.* Oct. 31, 2001. <http://www.theregister.co.uk/content/4/22579.html>.

Tenet, G. Statement before the U.S. Senate Foreign Relations Committee, March 21, 2000.

"Toulouse Explosion May Have Been a Terrorist Attack." *USA Today.* Oct. 4, 2001. <http://www.usatoday.com/news/sept11/2001/10/04/toulouse.htm>.

"Tunisia Synagogue Toll Rises to 7." CNN.com. April 12, 2002. <http://www.cnn.com/2002/WORLD/africa/04/12/tunisia.toll>.

"'Unpredictable' al Qaeda Blamed in Bali." CNN.com. Oct. 15, 2002. <http://www.cnn.com/2002/WORLD/asiapcf/southeast/10/14/bali.alqaeda>.

U.S. Fire Administration (USFA)/Federal Emergency Management Agency (FEMA). "Emergency Response to Terrorism: Basic Concepts." Seminar. Washington, DC: USFA/FEMA.

U.S. House of Representatives. U.S. Code: Annual Country Reports on Terrorism. Title 22, Section 2656f(d). Washington, DC: U.S. House of Representatives.

Violence Policy Center. "Sitting Ducks: The Threat to the Chemical and Refinery Industry from 50 Caliber Sniper Rifles." Washington, DC: Violence Policy Center, 2002. <http://www.vpc.org/studies/ducktwo.htm>.