

REMOTE

Site & Equipment Management

June/July 2004 Volume 4, Issue 3

a webcom publication

The Homeland Security Advisory System: Providing a Framework for Business Security

By Donald Schmidt
Risk Consulting Practice, Marsh Inc.

In response to the events of September 11, 2001, the U.S. government reorganized multiple departments into the new Department of Homeland Security and appropriated billions of dollars for preparedness and response purposes. Recognizing that terrorism is a threat to all sectors of American society, the U.S. government has extended the responsibility of preparing for, and deterring against, terrorist activity to states, local governments, and the private sector.

To provide a framework for this new approach to security, the Attorney General, in coordination with the U.S. Department of Homeland Security, developed the Homeland Security Advisory System (HSAS). The color-coded system is designed to alert government authorities, businesses, and the American public of a security threat according to a series of graduated conditions. The threat conditions range from low to severe and are dependent upon the threat's credibility, corroboration, imminence, and severity.

At each threat condition, the HSAS provides a set of corresponding protective measures. Federal government agencies are required to implement specific steps to reduce vulnerabilities at a

Key to our nation's security in times of crisis and considered to be likely targets for terrorism, critical infrastructure industries are required to implement specific security measures according to the HSAS.

particular threat condition. State and local governments are recommended to establish compatible systems. In addition, critical infrastructures - such as water treatment, telecommunication, and power and energy - are required to implement certain protective measures according to threat conditions.

As the government promotes preparedness across the country, workers are relying upon their employers for information and instruction on how to respond to security threats in the workplace. Over half of American businesses, however, are not ready for security-related risks. According to a 2003 survey by the American Management Association, only 64 percent of businesses have basic crisis management plans and 45 percent have specified plans for security threats. Moreover, only 42 percent of businesses conduct drills or simulations to test their crisis management plans. Regular exercises and evaluations are necessary to validate the effectiveness of an emergency response plan. Executives who install a plan but fail to train employees appropriately may have a false sense of preparedness as a result.

Many businesses are unprepared for security threats because of costs associated with changing or expanding emergency response, business continuity, and crisis management plans. According to the Center for Strategic and International Studies, raising the alert status from yellow to orange costs the government \$1 billion a

week. Unlike the government, however, businesses can actually reduce costs by implementing comprehensive plans to respond to terror alerts. Now more than ever before, insurance carriers are considering the scope of emergency response plans to determine placement terms, conditions, and pricing, particularly for high-value facilities or facilities - such as high-rise buildings and stadiums - where a large number of people gather. By employing a business continuity plan commensurate with HSAS threat conditions, businesses can also gain a competitive advantage. Business continuity plans enable organizations to maintain daily operations and fulfill customers' needs during high-level security threats. Moreover, vendors and suppliers are able to work confidently with organizations that have business continuity plans in place.

In addition, businesses must comply with regulatory requirements promulgated by the Occupational Safety and Health Administration (OSHA) of the U.S. Department of Labor and state and local fire prevention and life safety codes. For example, OSHA currently requires businesses to establish basic emergency response procedures. Recent legislation suggests that plans must be expanded to address preparedness for terrorism. Nevada's 2003 anti-terrorism bill, for example, requires resort owners to file their emergency response plans with local authorities and the state's Division of Emergency Management. Since most businesses should already have a basic emergency response plan, they can prepare for potential regulation changes by adapting it to security threats.

One key to effectively mitigating and even preventing security threats in the workplace is customizing the HSAS to individual businesses. A high-rise office building, for example, faces different risks than a chemical plant. Each building or facility should conduct a risk assessment to understand vulnerability to terrorism, potential consequences of an attack, and mitigation opportunities. The vulnerability assessment should address the many forms of terrorism including cyber attacks and the use of explosive, chemical, biological, and/or radiological weapons.

The risk assessment should also address the adequacy of emer-

gency response, business continuity, and crisis management plans and how preparedness should be enhanced for each of the five color-coded threat condition levels. Plans must be specific to building or site characteristics, population, nature of operations, and availability and capability of internal and external resources. Organizations should also define roles and assign responsibilities to employees at every department for each threat condition to effectively prepare their business, people, and property.

There are basic guidelines organizations can follow to prepare for security threats and appropriately respond to the HSAS. The accompanying sidebar suggests actions for businesses to take at each threat condition of the HSAS. Businesses should customize these suggested actions to fit the needs of their operations, people, and property. Consultation with risk management advisors, human resources personnel, and counsel is recommended. The guidelines range from coordinating emergency response plans with local

Color	Threat Condition	Protective Measures
Green	Low	<ul style="list-style-type: none"> ■ Conduct or update vulnerability assessments to determine potential exposure to terrorist incidents including cyber attacks. Survey the surrounding area to identify neighboring facilities (e.g., government buildings, industrial facilities, transportation routes or facilities) that are potential terrorist targets and would impact the site, if attacked. Employ mitigation strategies, where practical. ■ Review physical and operational security to ensure it is commensurate with the needs of the facility. ■ Review emergency response, business recovery, and crisis management plans and identify updates required by changes in physical conditions, personnel, or potential impact on employees or business operations. Review protective actions, including evacuation and shelter-in-place plans and review scenarios where each strategy would be employed. Update plans as necessary. ■ Establish early-warning systems to quickly learn of potential threats and provide a means of warning employees to take protective actions in the event of an emergency. Coordinate emergency preparedness activities with local public officials. ■ Conduct training, education, and drills as required by local, state, and federal regulations and as necessary to familiarize personnel with site emergency procedures. ■ Conduct annual exercise to validate plans, generate awareness, and educate members of your response and recovery teams.
Blue	Guarded	<ul style="list-style-type: none"> ■ Include all measures from Green level. ■ Inspect exterior lighting, fences, door and window locks, surveillance equipment, and intrusion alarm systems and verify they are in good condition. ■ Inspect and test all fire protection, life-safety and alarm or communication systems used to alert building occupants to take protective actions as well as systems used by emergency response and recovery teams to communicate during an emergency. Verify communication links to official government information are open and monitored. ■ Verify that members of emergency response, business recovery and crisis management teams have access to latest copies of plan documents; are familiar with their roles and responsibilities therein, and verify all critical personnel can be contacted 24 hours a day, seven days a week.

authorities, utilities, and community leaders at a low level alert to restricting access to workplace areas and facilities when there is a severe risk of attack.

In addition to these general guidelines, many trade associations have developed industry-specific homeland security preparedness guidelines that address emergency response, business continuity, and crisis management planning.

Energy, transportation, telecommunications, and financial services are industries considered to be part of our nation's "critical-infrastructure." In fact, 85 percent of telecommunication and information service providers, transportation companies, energy and water suppliers, and other critical industries are privately owned. Key to our nation's security in times of crisis and considered to be likely targets for terrorism, critical infrastructure industries are required to implement specific security measures according to the HSAS.

In addition to the nation's critical infrastructure, businesses in a variety of industries may be exposed to terrorist threats and security-related risks that vary according to location and operation. As a result, they need to customize security procedures, accordingly. Businesses with operations located in or near areas that might be considered at greater risk for terrorism, such as shopping malls, high-profile office buildings, and city landmarks, should take steps to assess their security practices and preparedness as well. Hotel, lodging, and convention facilities, for example, face unique security challenges because they encounter a constant flow of guests, vendors, deliveries, and vehicles that vary on a daily basis. Due to the nature of their business, hotels, lodges, and convention centers must adopt security measures to control and track the influx of visitors, luggage, and packages to detect and deter any suspicious activity.

Establishing information-sharing systems is one low-cost way businesses in a number of industries have enhanced their security practices. More than a dozen industry-specific information sharing

Color	Threat Condition	Protective Measures
Yellow	Elevated	<ul style="list-style-type: none"> ■ Include all measures from Green and Blue levels. ■ Secure buildings and storage areas not in regular use. Increase frequency of inspections and patrols within the facility. Close and lock doors and barriers except those needed for immediate entry and egress. ■ Scrutinize all contractors, visitors, and packages entering the building. Use company- or government-issued photo ID's to verify identity. ■ Consider restricting access of motor vehicles to those driven by identifiable employees and scheduled deliveries only. ■ Randomly inspect vehicles and packages entering the site or building, if the facility is considered a terrorist target. ■ Remove or prevent access to waste containers or areas that could be used to hide an explosive device or terrorist weapon. ■ Increase exterior surveillance to identify suspicious activities or packages. Report the presence of unknown persons, unidentified or suspicious vehicles, abandoned parcels or packages, and other suspicious activities. ■ Maintain adequate complement of security personnel to maintain high level of surveillance and staff assigned to emergency functions. ■ Request that public law enforcement authorities increase the frequency of patrols for unguarded facilities. ■ Constantly monitor radio, television, or other official communication channels to ensure prompt receipt of warning or threat information.
Orange	High	<ul style="list-style-type: none"> ■ Include all measures from Green, Blue, and Yellow levels. ■ Provide enhanced security to prevent penetration of site perimeter. ■ Consult local authorities about restricting the use of public roads, walkways, or entrances/exits to public transportation systems that might make the facility more vulnerable to terrorist attack. ■ Erect barriers to control the direction of travel and proximity of motor vehicles; restrict parking in proximity to buildings or other sensitive areas. ■ Screen access to all public areas; prohibit access of unauthorized persons. ■ Randomly inspect vehicles and packages entering the site or building, if inspections are not already conducted. ■ Provide staffing necessary to cover all unsecured points of entry. ■ Place all members of emergency response, business recovery, and crisis management teams on alert to respond immediately, if called. ■ Verify that emergency operations centers and business recovery sites are properly equipped and ready for occupancy, designated staff are prepared to occupy the site to carry out emergency plans, and non-essential staff are directed to work from alternate sites or from home, if and as directed. ■ Emergency plans should be up-to-date; staff should be briefed regularly. ■ Emergency procedures drills should be conducted as needed to ensure prompt decision making, notification, and execution of evacuation and shelter-in-place protective actions.

systems exist in the U.S. today, including the North American Electric Reliability Council, Coordinating Center for Telecommunications, and Association of Metropolitan Water Agencies. These organizations serve as information resources on various security-related topics for their members. In addition, with the goal of elevating awareness to industry-specific security threats, general industry businesses have organized themselves in non-profit associations, such as The Real Estate Roundtable and The Financial Services Roundtable, to create a partnership between industry professionals and government agencies.

Professional roundtables and information sharing centers offer a starting point for businesses to assess, develop, and improve emergency response, business continuity, and crisis management plans. While cooperation at the industry-level contributes to security in the workplace, preparedness for security threats at the local business level is still considered to be the most effective way to protect business employees, customers, operations, and property.

Established just over one year ago, the HSAS has not erased our vulnerability to terrorism, but it has provided us with a framework to prepare locally for terrorism, and the direct involvement

Red	Severe	<ul style="list-style-type: none"> ■ Include all measures from Green, Blue, Yellow, and Orange levels. ■ Monitor radio and television to receive official instructions or orders from public authorities; prepare to release non-essential employees and close facilities as directed by governmental authorities ■ Activate and execute emergency response and business continuity plans specific to the location and nature of any incident. ■ Take all appropriate actions to safeguard personnel safety and health. ■ Consider restricting access to the site or important buildings to essential and authorized staff only. ■ Inspect all vehicles entering the site to detect possible weapons. ■ Remove from proximity to the building all vehicles whose owners have not been identified. ■ At important facilities, increase the frequency and scope of security patrols to the maximum level sustainable. ■ Frequently communicate with members of emergency response, business continuity, and crisis management teams to relay official information, assess staffing and readiness levels, and execute pre-determined plans immediately, if warranted. ■ Activate crisis management plans to evaluate and address any impact; communicate with staff and key stakeholders as needed. ■ Make available employee assistance programs to address human impact.
-----	--------	--

of businesses has proven to be more vital than ever before. Conventional safety plans sufficed for fires and floods, but terrorism requires a new and heightened awareness and preparedness among all types of businesses and government entities.

Donald Schmidt is Senior Vice President and the Practice Leader of Marsh's Emergency Response Planning consulting practice. Contact Marsh at www.marsh.com