GETTING READY

Company Primer on Preparedness and Response Planning for Terrorist and Bioterrorist Attacks

Business Executives for National Security

Revised January 2007

Company Primer

on

Preparedness and Response Planning

for

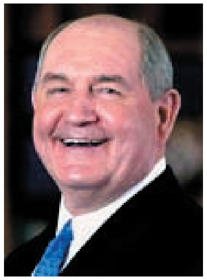
Terrorist and Bioterrorist Attacks

Change Do Solve Work Drive Act Team

Business Executives
for National Security

Prepared by
Business Executives for National Security
Metro Atlanta Region

STATE OF GEORGIA
CONSTITUTION
WISDOM JUSTICE MODERATION
1776
DEPARTMENT OF PUBLIC SAFETY



Foreword by Governor Sonny Perdue

“Getting Ready” is the result of an innovative partnership between the State of Georgia and Business Executives for National Security (BENS). Why is such a partnership necessary? Because neither government nor business alone can succeed in protecting our nation from terrorism. Homeland security is everybody’s responsibility and the business community has a critical role to play. “Getting Ready” is an excellent first step. This document will help make us more secure by helping businesses become better prepared.

BENS President and CEO, Gen. Chuck Boyd, U.S. Air Force (Ret.), and I announced our partnership in October 2003. Since our joint announcement, BENS, working closely with my Director of Homeland Security, is helping local, state and federal agencies to address critical homeland security needs.

BENS is a primary channel for applying the business community’s expertise and resources to improve our homeland’s security. Only by working together will we secure our nation’s citizens. I congratulate the BENS Metro Atlanta Region and the State Government team that produced this very valuable primer.

Sincerely,

Sonny Perdue

Sonny Perdue

TABLE OF CONTENTS

EXECUTIVE SUMMARY

What should ***you*** do to protect your employees, your organization, and its stakeholders from a terrorist attack?

Employees, and the public, assume that businesses are being proactive in working with government agencies to develop adequate health and safety programs, crisis prevention plans, and post-incident response systems that address the myriad of risks that exist in today's world. Corporate emergency preparedness and response initiatives are becoming commonplace, where procedures regarding the safety of all employees are an integral part of overall company policy.

The U.S. Federal Court recently ruled that terrorism is a "foreseeable risk." In a separate case, the Port Authority of New York and New Jersey was found "negligent" in safeguarding the World Trade Center before the first terror attack in 1993. The result of these two rulings is that companies can be held liable if they cannot demonstrate that they have taken reasonable actions to prepare for, and respond to, a terrorist attack. Supporting these findings is the recent addition of insurance for terrorism, which is now available to corporations (see Section 4.8 below).

As a business leader, emergency preparedness is clearly important, and you should be personally involved. Companies have a legal, ethical, and moral responsibility to mitigate against the risk of a terrorist act and to prepare for the possibility of this event. If an incident occurs, it is in your organization's best interest to rapidly and smoothly respond to, and recover from, the event with a focus on saving lives and property and continuing operations.

The legal concern mentioned above is further supported and federally mandated if your organization is eligible to receive funding for emergency preparedness and response initiatives, such as an airline, a maritime port, a shipper, or a utility. But even if you are part of an organization that does not qualify for federal emergency preparedness assistance, you are responsible for the safety and security of your employees and for knowing how to act as part of a community response to an emergency situation.

Homeland security is everyone's business. This primer will help you and your company to understand the threat of terrorism and its different types, to recognize attacks, and to prepare for, respond to, and recover from an emergency situation. It will also provide some useful links to other homeland security-related resources.

Companies have a legal, ethical, and moral responsibility to mitigate against the risk of a terrorist act and to prepare for the possibility of this event.

Based on feedback from its private sector membership after the September 11 attacks, the Business Executives for National Security (BENS) Chapter in the metro Atlanta area found that companies of all sizes need guidance on what constitutes an emergency preparedness and response plan (EP&R) for potential emergency situations. The EP&R is much more than a traditional continuity of operations plan: it focuses on all elements of the emergency management cycle (mitigation, preparedness, response, and recovery). This company primer is intended to raise the awareness of company leaders about terrorist threats, as well as other all-hazard emergencies, and to provide policy and procedural guidance for the development of overall corporate EP&R plans, policies, and procedures.

Specific information in this primer includes:

- The scope and scale of terrorism and the possible types of attacks.
- How to recognize a potential terrorist attack, including basic procedures you can put into place to rapidly identify hazards on or near your premises
- How to prepare for potential emergency situations, including:
  - initial threat and vulnerability assessments
  - checklists for critical elements of EP&Rs
  - facility preparation plans and response policies
  - employee training and simulation/drill exercises
  - family/personal disaster readiness
  - crisis communications procedures for notifying your employees of an event and assisting your executives in dealing with the media and the public
- Procedures for responding to a terrorist attack, including the crucial importance of rapid interaction with local officials to save lives and property
- How to recover from the event, including continuity of operations and post-incident issues related to your employees and other key relationships

Though many of the emergency preparedness & response guidelines are specific to terrorism, these plans can easily be adapted for preparing for and responding to other emergencies, such as fires, hurricanes, tornadoes, earthquakes, floods, power outages, public health emergencies (e.g., pandemic influenza), and even workplace violence. Companies should plan for a variety of incidents and must understand the governmental framework in place to respond to terrorism, as well as natural, man-made, and technological hazards. For example, while it is commonly known to contact local law enforcement for an incident of workplace violence, a terrorist attack with a biological agent requires that the local (county) health department be the first agency to be notified. Businesses need to know all of their local first responder organizations and to understand which officials should be called upon to respond to specific emergency incidents.

With that said, this primer will focus primarily on terrorism and is intended to help corporations develop an awareness and understanding of potential risks, begin to address these issues, and develop a closer dialogue with government agencies responsible for combating terrorism in all its forms.

This primer will be reviewed and updated on a consistent basis. We recommend visiting the BENS web site (http://www.bens.org) for the latest version. In addition, the appendices provide web site links to a variety of local, state, and national resources where additional information on this topic may be obtained. As a business executive, we urge you to pass this primer along to your safety director, personnel/human resources manager, business continuity manager or other individuals responsible for corporate security to help them develop, establish, and activate your EP&R plans.

1.0 INTRODUCTION

Recent Terrorism Incidents Prior to 9/11

1993:	World Trade Center bombing, New York City
1995:	Subway system sarin gas attack, Tokyo, Japan
1995:	Alfred P. Murrah Federal Building bombing, Oklahoma City
1996:	Khobar Towers bombing, Dhahran, Saudi Arabia
1996:	Centennial Olympic Park bombing, Atlanta, Georgia
1998:	U.S. Embassy bombings, Kenya and Tanzania
2000:	U.S.S. Cole bombing, Aden, Yemen

September 11, 2001 focused the attention of the nation on the impact of a terrorist attack in a major metropolitan area. The anthrax attacks that followed in October 2001 demonstrated that terrorists could reach any size and type of organization in the United States. The recent use of improvised explosive devices (IEDs) on the transit systems in Madrid and London further indicate that terrorism is an international problem that can occur anywhere.

There is a real possibility that your company may become the target for a terrorist attack. This requires organizations to consider and develop programs to reduce their vulnerabilities and to develop explicit response plans in the event the company itself (or the surrounding area) is attacked. These emergency preparedness and response plans (EP&Rs) should address evacuation and shelter-in-place options, employee health and safety, emotional distress, and a plethora of business continuation issues.

Your company may become the target for a terrorist attack.

In response to these events, Business Executives for National Security (BENS) solicited input from its members about what would constitute a guidance document for companies in developing EP&Rs for potential future terrorist attacks. BENS then began to work with both government health and safety officials and select members' firms to begin to address these planning concerns.

The result is this primer, structured to provide a brief overview of the scope, scale, and types of threats that face our nation, tips for how to recognize an attack, and guidelines for how to prepare for, respond to, and recover from an attack.

Your business has a legal, ethical, and moral responsibility to be prepared for terrorism. This primer is designed to further your understanding of the issues.

2.0 SCOPE AND SCALE OF TERRORIST THREATS

September 11 provided a stark example of the ability of terrorist groups like al-Qaeda to cause mass casualties on American soil and significantly disrupt the flow of goods and services. However, the 1995 Oklahoma City bombing demonstrated that these threats can come from domestic sources just as easily as foreign ones and can impact business and government anywhere in America. Thus, companies must prepare for potential terrorist attacks not only by well-financed groups on an international scale but also by a wide range of radical or fringe elements seeking to gain attention or further their agendas through acts of destruction.

In addition, companies cannot rule out emergency situations that result from irrational acts of vandalism or terrorist-type attacks by disgruntled employees or ex-employees or groups with which the company comes in contact in its normal course of business. Since the mid-1990s, companies have been aware of the need to ensure that their computers and electronic files are secure against hackers. Today, protecting these valuable electronic records and files against major attacks by cyber-terrorists is a necessity. The reality is that no company, regardless of size, is immune to disruptive and dangerous terrorist attacks.

Given the above, businesses must focus on the potential for terrorist activities and develop systematic plans and procedures for workplace response. Companies cannot rely solely on law enforcement agencies to protect them from such attacks; instead, company managers must incorporate in their business practices steps to increase awareness of, monitoring for, and security against attacks at or near the workplace.

The U.S. Department of Homeland Security recommends an all-hazards approach to emergency preparedness.

The good news is that your efforts to prepare for and respond to terrorism will also apply to natural hazards. As clearly demonstrated by the recent hurricane damage on the Gulf Coast, the prevalence of tornadoes across the Midwest, the summertime wildland fires in the Mountain West, and the earthquake probabilities on the West Coast, it is possible that your organization will one day face a natural emergency situation.

This primer (as well as the U.S. Department of Homeland Security) recommends an all-hazards approach to emergency preparedness. Given that it is more likely that your company will face a natural or non-criminal emergency, such as pandemic influenza, it is good to know that the basic premises within this primer apply to any type of hazard your organization may face.

3.0 HOW TO RECOGNIZE A POTENTIAL TERRORIST ATTACK

3.1 Recognizing the possibility of an attack

3.1.1 Absenteeism or other unusual patterns

As employers, businesses provide a vital window on the health status of a community. For example, a covert or unannounced release of a biological pathogen may cause an illness that first manifests as increased absenteeism in the workplace. Employers should be familiar with the sick-leave patterns of their employees and should ensure timely reporting to senior management when an unanticipated increase or unusual pattern develops.

It is important that businesses, in turn, report unusual patterns of absenteeism to their local public health department (or to a local government official in communities that do not have a public health department presence). All states are actively developing emergency preparedness and response plans for terrorist and other catastrophic events with the help of federal funding. One of the elements in many state plans is a “sentinel” program, through which local health departments and the states can effectively assimilate and analyze early signs indicating the possibility of a bioterrorist attack. An unusual or high incidence of absenteeism in the workplace is one useful piece of information in making these assessments.

Report unusual patterns of absenteeism to the local public health department.

3.1.2 Mailroom procedures for managing suspicious packages

Because all businesses receive mail, and because it is relatively easy to send explosives (letter bombs) and/or biological agents (such as anthrax) through the mail, companies should develop specific procedures for managing suspicious packages. Employees need to be educated about recognizing suspicious packages and know the procedures to follow if they receive such a package. Emphasis should be on minimizing exposure (unprotected contact between employees and the suspicious package) and timely notification of appropriate authorities. Following are some of the common warning signs of mail and packages that might indicate a terrorist or bioterrorist parcel:

- Unexpected mail, or mail from someone unfamiliar to you
- Addressed to someone no longer with your organization
- Excessive postage
- Handwritten or poorly typed address
- Homemade labels, or cut-and-paste lettering
- Incorrect titles
- Title, but no name
- Misspellings of common words

- Oily stains, discolorations, or strange odors
- No return address, or a return address that cannot be identified as legitimate
- A city or state in the postmark that doesn't match the return address
- Restrictive endorsements, such as "Personal," "Confidential," "Fragile," or "Rush"
- Oddly shaped, has bulges or soft spots, or is an unusual weight for its size
- Protruding wires
- Dripping powders or liquids
- Package makes a buzzing, ticking, or sloshing sound

Keep in mind that a bomb or biologically-tampered package can be enclosed in either a parcel or an envelope, and its outward appearance is limited only by the imagination of the sender. However, mail bombs have some unique characteristics which may assist you in identifying a suspect mailing. To apply these factors, it is important to know the type of mail your organization normally receives. Do not hesitate to suspect a piece of mail or package that is out of the ordinary.

If a parcel appears suspicious, the following are important steps to take:

- Isolate the parcel and handle with care
- Do not open, smell, or shake the parcel
- Do not place the parcel in a confined space (e.g., filing cabinet or desk drawer)
- Call the police (9-1-1)

3.1.3 Security procedures for building ventilation (HVAC)

The release of a biological agent into the ventilation system of a building could pose a considerable threat. Given that a terrorist action of this nature is likely to be covert, and large numbers of people could be exposed to a biological agent in a very short period of time, businesses should closely evaluate their security pro-cedures and physical vulnerabilities in this area. The following could be indicative of a bioterrorist release via a building's HVAC:

- Damage to HVAC intakes or other evidence of tampering
- Residue or discoloration in or near HVAC intakes
- Other indications of tampering with HVAC equipment
- Packages, briefcases, knapsacks, luggage, opened containers, etc. near HVAC

The following actions should be performed to minimize the possibility of such events:

- Inspect HVAC equipment and all intakes frequently
- Ensure that HVAC equipment is in a secure location
- Include the ventilation system as part of a hazard vulnerability assessment and in subsequent emergency response plans
- Define procedures for notifying local law enforcement, EMS, local emergency management agency, and local public health agencies regarding any perceived threat or indication of a bioterrorist event

4.0 TYPES OF TERRORIST ATTACKS

Not only could terrorists target almost any location, the attack could potentially come in a wide range of forms, depending on the means and objectives of the responsible group. The Oklahoma City bomber used a "homegrown" device comprised of fertilizer and diesel fuel. The Olympic bombing in Atlanta was an explosive device abandoned in a crowd. The September 11 hijackers turned commercial airplanes into deadly unconventional weapons for a destructive, mass-casualty attack. Officials fear terrorists are currently attempting to acquire and use weapons of mass destruction (WMD), including chemical, biological, nuclear, and radiological weapons ("dirty bombs"), for similar ends. Cyber-terrorism could be used to disrupt economic activity, sow confusion, or mask another type of attack.

Although any of the threats described above can create an emergency situation and cause significant disruption to our society and its normal functions, the biological attack is the least understood of these threats, and its manifestations are unfamiliar to the general public. Moreover, biological events may have certain characteristics that impose additional challenges. The event may be silently unfolding, escaping early detection. The scale of a biological event may be difficult to predict; there may be one or two victims, or the number of casualties may exceed thousands. Unlike other disasters limited to a single location, the biological disaster may spread as the disease is communicated from one person to another. The biological threat is considered to be one of the most likely forms to be used against a corporation.

Recent events in Europe indicate that an improvised explosive device (IED), carried and delivered in a piece of luggage or a vehicle, is also a common mechanism for a terrorist act. This device is difficult to recognize on a timely basis and can cause extensive damage to lives and property. The IED threat has proven to be one of the most likely forms used to attack a company.

To effectively respond to terrorist threats, the public (law enforcement and public health) and private sectors (the business community) will need to work closely together

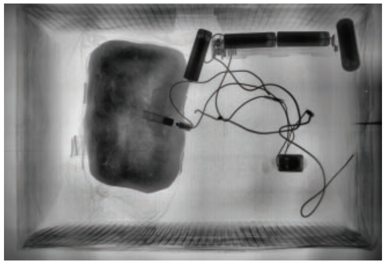
To effectively respond to IEDs, bioterrorism, and other types of terrorist threats, the public (law enforcement and public health) and private sectors (the business community) will need to work closely together, sharing information and resources. There are currently several federal initiatives to improve public-private sector collaboration, including the national focus on critical infrastructure protection.

4.1 Improvised Explosive Devices (IEDs)

Six of the seven major terrorist incidents that occurred prior to the events of

September 11 involved bombs utilizing conventional explosives. An improvised explosive device (IED) is a device built and placed in an improvised manner, incorporating destructive, lethal, and incendiary chemicals and materials. IEDs are designed to destroy lives and property and can be delivered via various methods such as luggage, vehicles, or packages/letters in the mail system.

Attacks on transit systems in Madrid and London utilized IEDs. IEDs also are responsible for many of the casualties suffered by U.S. and Coalition military forces in Iraq and Afghanistan. IEDs are also favored for use in domestic terrorism, as indicated in the attack by vehicle to the Murrah Building in Oklahoma City and also in the Columbine High School tragedy, where the perpetrators crafted 74 IEDs and set a diversionary explosion to draw away emergency responders.



An IED can be comprised of many different types of materials and activated through various methods. They can be produced in different sizes, functioning methods, and containers and can use commercial or military explosives, homemade explosives, or even military ordnance. Today's IEDs are primarily high-explosive charges, but there is a genuine threat that chemical, biological, or even radiological agents could be added by the terrorist to the IED to maximize the destructive power and psychological effect of the device.

IEDs typically fall into three types of categories:

- ***Package-Type***
  A package-type IED is an explosive device sent via the postal service (or another courier system). These devices are usually set to explode immediately on opening, with the intention of seriously injuring or killing the recipient (who may or may not be the person to whom the bomb was addressed).

- ***Luggage-Type***
  A luggage-type IED is an explosive device hidden within a piece of luggage, such as a book bag or rucksack. These devices are typically triggered by a timing device or at a remote distance via a cell phone or other transmitter. Some luggage-type IEDs are set to explode upon opening of the luggage.

- ***Vehicle-Borne***
  A vehicle-borne IED is a bomb that is placed in a car or truck. It is a favorite instrument of terrorists because the car bomb acts as its own delivery mechanism and can carry a relatively large amount of explosive without attracting suspicion.

IN THE EVENT OF AN IED ATTACK

- Primary rule: If a suspected device is encountered, it should not be handled and the area should be secured. Improvised explosive devices are very unstable. They are extremely sensitive to shock, friction, impact, and heat, and may detonate without warning. Even the smallest devices can cause serious injury or death.
- Secondary rule: Always assume that there is more than one device present, whether it is a bombing, a threat, or a device that has been located.
- Package-type IEDs: Institute security procedures in your company's mailroom and instruct employees on how to recognize suspicious packages.
- Luggage-type IEDs: Train security personnel and employees regarding unattended packages of any type. Never pick up or open any suspicious package or piece of luggage. If an IED is discovered, call the appropriate law enforcement authorities; do not touch the device.
- Vehicle-borne IEDs: Perform a vulnerability/threat assessment for your facility with special attention to this type of explosive delivery mechanism. Consider the use of enhanced security away from your key buildings (such as a vehicle checkpoint) or the use of cement planters or jersey barriers to block vehicular access to building entrances.

4.2 Chemical Attacks

A chemical emergency occurs when a hazardous chemical has been released and has the possibility of harming people's health. While potentially lethal, chemical agents are difficult to deliver in deadly amounts. If released outdoors, the agents often dissipate rapidly. As such, the most lethal area for a chemical release is inside a confined space, such as a building, public place, or subway system.

Some hazardous chemicals have been developed by military organizations for use in warfare. These include nerve agents such as sarin and VX, blister agents such as sulfur mustards and nitrogen mustards, and choking agents such as phosgene. Supplies of any of these could be obtained through the underground munitions market or manufactured by a terrorist organization.

Industrial chemicals, while not as lethal, can be just as effective if released in sufficient quantities. Chlorine, ammonia, benzene, and other toxic chemicals are routinely transported through densely populated areas in rail tankers or truck tankers and could be the target of a terrorist attack.

Chemical terrorist attacks will most likely be overt because the effects of most chemical agents are immediate and obvious. Your response will have to be thought out and practiced in advance to be effective.

IN THE EVENT OF A CHEMICAL ATTACK

EVACUATION

Some types of chemical emergencies will require evacuation from the immediate area. If you are up-wind and in the open, evacuate up-wind and away from the incident. Cover your mouth and nose with a damp cloth. If you have been exposed, you will have to be decontaminated by first responders.

SHELTER IN PLACE

If you are already down-wind and/or in a multi-story building, you may be instructed to shelter in place or to make that decision on your own. Most likely you will only need to shelter for a few hours. The procedure includes:

- Go inside as quickly as possible shut and lock all windows and doors; turn off all HVAC equipment and any fans.
- If you have multiple floors, go as high as practical, three to five floors. (Most chemical agents are heavier than air.)
- If you have duct tape, tape over door and window cracks, vents, electrical outlets, and any opening to the outside.
- Wait for instructions from first responders before leaving.

DECONTAMINATION

First responders will direct and coordinate decontamination, if required. If you are sheltering in place and think you have been exposed to a chemical agent, it is important to decontaminate yourself and any others in the shelter.

Decontamination procedures include the following:

- Remove clothing (do not pull any clothing over your head cut it off)
- Anyone assisting should wear gloves, mask, and eye shielding, if available. Dispose the same in a separate plastic bag, plainly marking on the outside of the bag that it contains disposable items.
- Wash thoroughly with soap and water. If you wear glasses, wash them before wearing.
- If you wear contact lenses, dispose of the ones you were wearing during the event, irrigate your eyes for at least 30 seconds, and do not wear contact lenses again until evaluated by an opthalmologist or doctor of optometry.
- Dispose of all contaminated items in plastic bags and seal, plainly marking the bags that contain personal effects.
- Wait for instructions from first responders.

4.3 Biological Attacks

A bioterrorist attack could happen in any workplace in America, yet most company personnel know little about potential biotoxins or biopathogens or how to recognize these agents and respond in the event of an attack.

The Centers for Disease Control and Prevention (CDC) in Atlanta, Ga., defines “bioterrorism” as the illicit use of biological agents (e.g., bacteria, viruses, and parasites or their byproducts) to cause illness and spread fear. Bioterrorism could be intended to harm humans and other living organisms, to influence the conduct of government, or to intimidate or coerce a civilian population.

Certain biological organisms are better suited than others for use as weapons. This is due to the ease with which a terrorist can grow, acquire, and/or maintain adequate quantities of the organism; the ability to spread the organism to large numbers of victims; the ability of the organism; to spread from person to person once released; and the severity of the disease caused by the organism.

There are several ways a bioterrorist event may manifest itself. The biological event may result from a covert attack. A covert attack may be unleashed by the receipt of an object, such as a package or piece of mail, accompanied by a warning or threat. For example, release of a biological agent could occur through delivery of a package contaminated with anthrax spores or another pathogen. Biological agent release also could occur via the ventilation system (HVAC) in a building, where dispersal could take place within a matter of minutes. Because the covert release is not witnessed, the effects of such an event can be widespread and difficult to isolate or recognize. Exposed individuals might begin to visit ambulatory clinics and emergency departments two to seven days after the release of the agent and following the onset of symptoms. Because the early phase of these illnesses may have non-specific symptoms (e.g., fever, malaise), they are difficult to distinguish from other ordinary ailments, such acute respiratory or flu-like illnesses.

Alternatively, the attack may be an overt act, where the release of the pathogen into the environment is either announced or witnessed by persons present. In this scenario, a known or suspected pathogen is overtly released into the environment, causing exposure to a number of persons. In addition to securing the site to prevent additional human exposure, efforts would focus on identifying or confirming the pathogen involved and isolating persons suspected of having been exposed. It is important to note that a bioterrorist event could be committed in conjunction with another type of attack (e.g., cyber-terrorism), magnifying the terror effect or potentially masking the more deadly medical emergency that is about to unfold.

IN THE EVENT OF A BIOLOGICAL ATTACK

The goal of the medical care community (i.e., hospitals, physicians, and other health care providers) is to recognize and diagnose the disease (which frequently may be unfamiliar to most clinicians) and to provide treatment. The goal of public health authorities is to detect and control the outbreak of the illness. Public health officials will focus on identifying and treating exposed persons and preventing the spread of disease.

In response to a covert release, it is important for you, as an employer, to recognize the signs and symptoms of an emerging disease within your workforce. The initial indication may be related to absenteeism, with your employees presenting similar symptoms. Do not hesitate to contact your local public health authorities if you detect abnormalities in your workforce.

This action could also save lives. For some diseases (anthrax), control measures may include providing antibiotics to exposed persons. The antibiotics, if given soon enough after exposure, may prevent the occurrence of illness altogether or may make the illness less severe. For pathogens that spread from person to person such as smallpox, public health authorities may also consider quarantine.

If an overt release is recognized, take immediate action to isolate the exposed employees and/or area of agent dispersion and to remove others from the area of release. Notify your local public health authorities immediately and follow their directions. Decontamination may also be warranted in response to an overt release.

While terror is intended to produce casualties, disruption, and fear, the use of biological agents is particularly injurious. Biological attacks are delayed events. The sudden appearance of generalized symptoms in victims who present themselves to medical providers may initially disguise the true source of exposure. Only when a trickle of patients turns into a flood or mysterious pathogens quickly make their presence felt does the magnitude of the event reveal itself.

Biological agents are indiscriminate; whole populations are vulnerable within the areas impacted by a release. In most instances, time is of the essence.

Those exposed or considered at risk will require medications like antibiotics or, in the case of smallpox, inoculations. Mobilizing local, state, and regional health care for mass prophylaxes and vaccinations involves more human and material resources than local or state governments currently possess. The private sector, if properly positioned, can assist these efforts.

4.4 Radiological Attacks

A radiological weapon or “dirty bomb” is a crude device that combines a conventional explosive with highly radioactive material. When detonated, the blast vaporizes the radioactive material and propels it across a wide area. The main danger from a dirty bomb is the initial blast, which could cause serious injury or property damage. The radioactive materials will likely not be concentrated enough to cause immediate serious illness, except to those very close to the blast site or those who inhale smoke and dust. Dirty bombs are designed to cause tremendous psychological damage by exploiting the public’s fear of radiation. These are not weapons of mass destruction, but weapons of mass disruption aimed at wreaking economic havoc by making target areas uninhabitable for extended periods.

IN THE EVENT OF A RADIOLOGICAL ATTACK

There are three basic ways to reduce your exposure: (1) Time Reduce your time near the source of radiation, (2) Distance Increase your distance from the source of radiation, (3) Shielding - Increase the shielding between you and the source of radiation. Shielding is anything that puts distance and mass between you and the radiation source.

EVACUATION

If you are outside, evacuate up-wind from the blast site cover your nose and mouth with a wet cloth to reduce the risk of inhaling radioactive smoke or dust. Once you have left the immediate area, seek shelter and wait for instructions from first responders. If you think you have been exposed to dust or smoke, follow the decontamination instructions found under the chemical attack section.

SHELTER IN PLACE

If you are close to the blast and inside a building, stay inside if the building is intact. Move to the basement and turn off all HVAC equipment and fans bringing in outside air it is not necessary to tape doors and windows, but it may be helpful. Wait for instructions from first responders.

4.5 Nuclear Attacks

According to the Department of Energy and the Department of Homeland Security, nuclear terrorism is the number one security threat facing the United States. The nuclear threat differs from a radiological attack in that instead of an improvised explosive device as the delivery mechanism, the nuclear attack involves a large-scale dispersion of radiological materials from a nuclear bomb, in addition to massive blast and heat effects.

While many security experts consider a terrorist nuclear strike highly unlikely because of the difficulty in obtaining fissionable material, is nonetheless a conceivable scenario, especially in light of the lax security at many former Soviet nuclear facilities and the knowledge of atomic scientists in such places as Pakistan. Large quantities of fissile material exist around the world, and sophisticated terrorists could design and fabricate a workable atomic bomb if they managed to acquire the radioactive components.

The simplest nuclear weapons derive their energy from nuclear fission. A mass of fissile material is rapidly assembled into a critical mass, in which a chain reaction begins and grows exponentially, releasing tremendous amounts of energy. The dominant effects of a nuclear weapon (the blast and thermal radiation) are the same physical damage mechanisms as conventional explosives. The primary difference is that nuclear weapons are capable of releasing much larger amounts of energy at once, with intense light and heat, along with widespread radioactive material that can contaminate the air, water, and ground surfaces for miles.

IN THE EVENT OF A NUCLEAR ATTACK

What should you or your employees do in the event of a nuclear attack? If there is advance warning of the attack, seek cover as quickly as possible, going as far below ground as you can. Fallout shelters still exist in many communities, and you should be aware of their locations. If there is no warning, you can protect your employees via shielding (the denser and thicker the shielding, the less radiation passes through), distance (the further away you are from the blast, the radiation is less concentrated), and time (the less time spent in the contaminated area, the less the threat of health problems). Use available information to assess the situation. If you take shelter, go as far below ground as possible, close windows and doors, and turn off air conditioners, heaters or other ventilation systems. Stay where you are, watch TV, listen to the radio, or check the Internet for official news as it becomes available.

5.0 HOW TO PREPARE FOR A TERRORIST ATTACK

5.1 How an attack can affect business

Because the sizes, nature, geographic locations, procedures, and physical layouts of companies vary widely, it is impossible to develop a generic emergency preparedness and response plan that could effectively be used by all companies. In addition, most businesses are vulnerable to differing types of natural and man-made hazards, which should be addressed with hazard-specific EP&Rs.

Nevertheless, there are a number of common issues and elements that should be considered when developing an EP&R for a business entity. This section outlines some of the critical issues and elements of a preparedness and response planning agenda, including risk assessment, facility preparation and hardening, insurance issues, communications procedures, and employee disaster planning.

Most businesses are vulnerable to numerous types of natural and man-made hazards, which should be addressed with hazard-specific Emergency Preparedness and Response Plans.

Due to the varied forms a terrorist attack can take, most companies might never be affected by a direct attack but still could be severely impacted by degradation in basic services (such as mail, transportation, and communications) that result from an event within their community. Anthrax, for example, has proven to be particularly disruptive to the mail system, contaminating mail handling facilities and any office or business to which it is delivered. A coordinated attack could have devastating nationwide effects for mail delivery, including increased costs, long delays, lost mail, and potential restrictions on mail delivery.

Numerous other agents (chemical, biological, radiological, or explosive) could also be used, with probable targets being transportation hubs (airports, train/subway systems, or port facilities), central city areas, and areas with large population concentrations (stadiums, convention centers, or shopping malls). These attacks might be aimed at creating fear and terror in the population and/or contaminating the facilities to render them temporarily unusable. Businesses with strong public profiles or well-known political ties, and those in important locations (e.g., near critical infrastructure, in tall buildings, near federal offices), could be more attractive targets for an attack.

Businesses could be severely impacted by degradation in basic services (such as mail, transportation, and communications) that result from an event within their community.

Communication systems could also be targeted. Maintaining and/or reestablishing communications with local emergency response personnel, employees, customers, suppliers, and the community will be a major component of any response plan.

5.2 Hazard vulnerability / security assessment

In developing a site-specific EP&R, an assessment needs to be made of the vulnerability of a particular site or business. While the likelihood of a specific company or building being targeted for a terrorist attack is difficult to predict, a survey of some general risk factors can be a guide to a company's vulnerability and indicate how detailed an EP&R should be. Some of the risk assessment factors that should be considered include:

- Industry Is your company or facility a critical industry or part of a critical infrastructure sector (e.g., transportation, communication, power, water supply, health services, defense or banking)?
- Geography Is your facility located near other assets that provide critical services? These could include:
  - Transportation hubs or central structures bridges, tunnels, subways, airports, or maritime ports?
  - Refineries, chemical plants, storage facilities, or pipelines?
  - Nuclear/conventional power plants or major electrical switching centers?
  - Defense facilities: naval ports, air bases, logistic deports, command centers?
  - Specialized facilities: governmental centers, communication hubs, Federal Reserve banks, FAA control centers, national sites of significance?

Do you know your company's risk assessment factors?

Although not meant to be exhaustive, the above list illustrates some factors that may increase the risk profile of a specific company. A sample assessment is located in Appendix C on page 40.

5.3 Facility preparation and hardening

The following is a partial list of considerations to help prepare and harden your facility against a terrorist attack:

- Does the facility have a security system?
- Are parking areas monitored?
- Is outside of the building or workplace and parking lot adequately lighted?
  - Is a procedure in place to ensure light bulbs are checked and operating?
- Is landscaping around building neat and well kept (minimize hiding places)?
- Is the workplace locked when appropriate?
  - Are all doors and locks operating properly?
  - Are door closers properly adjusted to close doors after entry/egress?
  - Does the work facility have a security system?
  - Is the security system routinely used?
  - Is there a procedure in place to deny access to the workplace to ex-employees or unauthorized persons?

- Does the company have an adequate method of identifying all who work in or visit the facility?
  - Is access restricted in critical or sensitive areas?
  - Is access limited to only current employees and visitors?
- Have employees been trained and encouraged to be alert to and look for unusual packages, cars, or other signs of a suspicious event?
  - Is there a procedure for reporting any unusual activity or facility problems within the company?

5.4 Facility response options: shelter-in-place or evacuation

In the event of a chemical, biological or radiological attack, it may be necessary for employees and visitors to remain in your office building for an extended period of time. This shelter-in-place concept has some planning implications that are unique to these types of terrorist attacks:

- Identify suitable shelter-in-place areas where personnel are to congregate. These should be interior rooms in a building and be above ground level because some chemical and biological agents are heavier than air.
- Do the shelter-in-place locations have facilities and supplies stored for employees and visitors for a one- to three-day period (water, food, first aid, communications, etc.)?
- Can the shelter in-place areas be easily isolated from the exterior environment by shutting down the HVAC system and sealing doors, windows and vents?
- Have you made a survey of, and do you understand the operation of, the HVAC system(s)?
  - Are the air intake(s) secure or out of reach from ground level?
  - How does the HVAC respond to fire alarms or actual fire detection?
  - How quickly can the HVAC be shut down? Who knows how to shut down the system?
- Does the area or building have shower facilities for decontamination?

In some terrorist events, an evacuation may be ordered by local public officials. The evacuation must be included in your company's EP&Rs:

- If evacuation is the best option, do you have procedures in place to notify your employees and to proceed with an orderly evacuation of the premises?
- Have you performed an evacuation drill?
- Do you have an established method of communicating with employees and emergency response personnel, and have you tested your alert notification system? See Section 5.5 below for additional information on this topic.
- Do you have battery operated radios, lights, and cell phones?
- Have you designated a primary and alternate assembly location for your evacuees?

5.5 Communicating with employees and other internal communications in an emergency

In the event of a terrorist act or civil disaster, timely, accurate communications will be critical for the success and survival of a company. The following should be considered in developing a communications plan within the overall EP&R:

In the event of a terrorist act or civil disaster, timely, accu-rate communications will be critical for the success and survival of a company.

- Designate a crisis leadership team and establish policies and procedures for communications. Communicate only through this team or their designates.
- What and how will you communicate with your employees or their families? Will you have a hotline or website available for employees/family members to receive authorized information from your company?
- What and how will you communicate with your clients? (They will want to know if and how their businesses will be affected by your situation.)
- What and how will you communicate with your vendors? (They will want to know if and how their business will be affected by your situation and if they will be paid for goods and services provided.)
- Who will be the primary contact with the local and state public health and public safety agencies (to improve the response to an emergency on your premises)?
    - Has the company met with local public health, public safety, and fire department officials to discuss specific preparedness and response plans?
    - Have specific first responder agency contacts been identified?
    - Do the individuals tasked with communication responsibilities have the contact numbers of the agency personnel (e.g., office phone, fax number, mobile phone number, home phone number)?

5.6 Communicating with the media and the public during an emergency

An important part of the communications plan is a definition of what, when, and how you communicate with the media and the public during an emergency situation. To this extent, your organization should decide who is the best and most credible spokesperson for the company and assign that person as your media contact.

Designate the best and most credible spokesperson for the company as your media contact.

This person will decide how often the company will provide media updates, designate a specific location for media communications, and personally deliver the messages. Other employees should defer to the media contact if approached.

Crisis communication goals of the designated media contact include:

- Positive messages with a focus on action taking place
- Clarity in all messages delivered
- Consistency in all messages repeated

- Bias-free messages
- Correct any misinformation
- Include and involve local emergency management officials

5.7 Employee training and simulation/drill exercises

Employee training is a critical part of a successful corporate emergency preparedness and response plan. The EP&R should clearly define both employee roles and responsibilities in a response effort but also establish and monitor performance levels via training and regular simulation/drill exercises.

Exercises are conducted to evaluate an organization's capability to execute one or more portions of its EP&R. An exercise is a focused practice activity that places the participants in a simulated situation requiring them to function in the capacity that would be expected of them in a real event. Its purpose is to promote preparedness by testing policies and plans and by training personnel. Many successful responses to emergencies over the years have demonstrated that exercising pays huge dividends when an actual emergency occurs.

Employee training is a critical part of a successful corporate emergency pre-paredness and response plan.

A 1989 plane crash in Sioux City, Iowa, provided a clear demonstration of the value of training and exercises. In July of that year, United Airlines Flight 232 crashed in flames after a failed emergency landing attempt. Although 109 lives were lost in this terrible disaster, 186 passengers survived. Their survival was due mainly to three factors:

- Response of the flight crew before the crash
- Trained rescue units waiting on the ground
- Centralized communications among all participants

These factors were present because of training, and the high level of training was no coincidence. Years before the crash, a disaster services center was established. Representatives from 40 organizations (both government agencies and private companies) met regularly to review employee emergency procedure training and plan realistic exercises.

5.8 Terrorism Insurance as a form of preparation

In the aftermath of September 11, insurance companies excluded terrorism risks from their commercial policies. The Terrorism Risk Insurance Act (TRIA), signed into law by President Bush in November 2002, required insurance companies to offer insurance for certain acts of terrorism in the U.S. that are "certified" by the Secretary of Treasury, the Secretary of State, and the Attorney General. The terrorism coverage offered under TRIA has to be in amounts and have terms and conditions that do not differ materially from other typical policies. In other words, a loss would neither be excluded nor covered just because it was caused by an act of terrorism. The act also requires insurers to disclose to policyholders the premium charge for providing such terrorism coverage.

As a complement to certified TRIA coverage, insurers are also offering "non-certified" coverage, which includes coverage for terrorism risks outside the U.S. as well as for terrorism in the U.S. arising from indigenous acts. As a third alternative, businesses can purchase separate, "stand-alone" terrorism insurance policies that are outside of their property insurance programs and do not require U.S. government certification.

A 2005 report published by Marsh Inc., based on data compiled from 2,371 businesses and government entities that purchased or renewed property insurance policies in 2004, found that "take-up" rates (the percentage of companies buying the additional coverage) varied considerably by region: about 53% of firms in the Northeast and Midwest purchased property terrorism insurance in 2004, compared with 47% in the South and 34% in the West.

Since its enactment, TRIA has helped stabilize the terrorism insurance market, making coverage for this risk more available and affordable. Its extension through Dec. 31, 2007, for now forestalls a situation in which the stand-alone insurance market would be unllikely to have sufficient capacity to satisfy all of the expected demand at commercially viable prices.

Business executives should be aware of TRIA provisions along with the other terrorism insurance options available and carefully consider whether it is prudent to purchase some form of terrorism insurance coverage as part of their company's preparedness and response planning program.

Do you have proper coverage for crisis situations?

5.9 Family/personal disaster readiness

This is a very important area to address within your company's EP&R plans. Why? Quite simply: In an emergency situation, your employees will be thinking first of the health and safety of their families and of their own personal safety. If your employees are aware of, and have prepared their families for, a potential terrorist attack, they will be more likely to show up for work, thus reducing continuity of operations issues for your organization.

Some state health departments are planning and developing "in-home hospitalization kits" which may be sent to families early in some events of public health significance. Businesses are encouraged to contact their local public health agency for additional information and assistance.

The American Red Cross offers a wealth of information on personal and family readiness, including disaster kits, family communication plans, and both evacuation and shelter-in-place information. Note that disaster kits (also called emergency response kits) should be available for your employees in case of a shelter-in-place situation. These same kits should be a part of your employees' personal disaster preparedness at home. Please refer to http://www.redcross.org and click on the "Get Prepared" link for this critical information. Additional details can be found at the DHS "Ready.gov" web site: http://www.ready.gov/america/index.html.

5.10 Familiarity with your local emergency management system

Timely notification of authorities requires employers to be familiar with how their state and local public health agencies and emergency management systems operate. Inviting local officials to speak at chamber of commerce meetings and other gatherings of business leaders can foster relationships between the business community and local emergency management officials.

Fostering relationships between the business community and local emergency management officials is critical.

Because an effective response to a terrorist event requires action by multiple agencies and response sectors, an essential element of preparedness is the development of relationships and familiarity with operating procedures across all sectors. Procedures for coordination, command, and communication must be established in advance if all the goals of the disaster response are to be met in a timely and effective fashion. Business leaders need to know their emergency response agencies and personnel and how their organization fits within a community-wide response effort.

5.10.1 Local, state, and federal relationships

In most states, the local jurisdiction (typically the county) has responsibility for emergency management and response. Often this authority is delegated to an emergency management agency. Most jurisdictions have a state and federal mandate to adopt the incident command system (ICS) to control and manage a coordinated response to a terrorist event. The ICS provides a robust management system for responding to all types of emergencies and terrorist attacks. Mutual aid agreements between local, state, and federal agencies enable effective coordination and sharing of resources across boundaries, particularly in the event of a crisis.

Business leaders need to know how their organization fits within a community-wide response effort.

When the disaster response outstrips local resources or involves multiple jurisdictions, the local emergency manager seeks assistance and coordination at the state level. When state capacity is exceeded, the governor, often through a state emergency management agency, seeks federal assistance from the Department of Homeland Security's Federal Emergency Management Agency (DHS/FEMA). The ICS is used by DHS/FEMA along with four basic principles of emergency management (mitigation, preparedness, response, and recovery). These systems are advocated by DHS/FEMA for use in emergency preparedness and response initiatives related to all types of emergency situations. For additional information, go to http://www.training.fema.gov.

In the event of terrorism, these basic local-state-federal relationships apply. Presidential Decision Directive (PDD) 62 and PDD 63 stipulate that in the event of a terrorist attack, the Federal Bureau of Investigation (FBI) will take the lead role for "crisis management" or issues related to preventing or responding to acts of terrorism. At the federal level, FEMA has lead responsibility for consequence management. During a bioterrorist attack, however, the local public health agency usually retains overall responsibility for command and control of emergency operations, except where state or federal statutes transfer authority to a specific state or federal agency. Thus, mutual-aid agreements among local jurisdictions remain in effect, as do any any existing arrangements for providing assistance between a state government and its localities. Similarly, if the state requires federal assistance for consequence management, DHS/FEMA maintains lead responsibility for coordinating assistance. DHS/FEMA is also responsible for providing aid to states and local agencies through the National Response Plan; this plan defines how the federal government will provide assistance in the event of a presidential declaration of emergency.

Business leaders should contact their local emergency management officials to understand their role within the Incident Command System (ICS) at the local level.

Although these multiple layers and roles make the emergency response seem complex and hierarchical, in practice the local, state, and federal agencies closely coordinate and mutually support each other's activities.

5.10.2 Special powers under a public health emergency (bioterrorism)

In the event of a bioterrorist event, the local jurisdiction (e.g., county executive officer, mayor, or other chief elected official), in concert with the local health authority, may declare a public health emergency. Under these circumstances, the local health authority may exercise those powers vested under such a declaration. Similarly, a governor may declare a state of public health emergency, thereby invoking, within the limitations of the state statute, broad exercise of power to address the emergency situation.
These special powers may be invoked during a state of public health emergency to manage the emergency and control property. Examples of where these powers might be needed specifically in the event of a bioterrorist attack include requirements to manage and control:

- Distribution of health care supplies (e.g., antibiotics and vaccines)
- Use and distribution of material and supplies
- Stressed medical resources and facilities (e.g., clinics and hospitals)
- Access to health care facilities (e.g., to prevent unruly mobs descending upon emergency departments seeking medications)
- Safe disposal of infectious waste and human remains
- Fair compensation of property seized for state purposes under emergency circumstances (e.g., the government uses a private facility as an infirmary to treat or isolate patients)
- Necessary destruction of property (e.g., nuisance abatement).

If relationships between the private and public sector have been established, a business will know who to call when something unusual occurs. Business managers, sensing something unusual in the absenteeism pattern of employees, will know to call the local or state health department. Employees and their supervisors will know to call appropriate public safety officials and public health officials for consultation and advice when a suspicious package arrives.

Time is a key element of an effective response. Therefore, a business not only needs to know "who to call" but how to do so promptly.

Time is a key element of an effective response. Due to the nature of biological agents, hours, even minutes, can make a significant difference in the ability to isolate and contain the event. Therefore, a business not only needs to know "who to call" but how to do so promptly.

Once again, employers need to be familiar with how their local and state emergency management systems operate. In addition, your organization may be able to play a significant role in responding to a community-wide event (e.g., by providing volunteers or physical assets to the response effort); as such, knowledge of and communication with your governmental counterparts are essential.

5.10.3 Overall checklist of issues for preparedness and response plans

A checklist provides a useful guide of items to consider when preparing an EP&R. Please see below the checklist from the National Business Group on Health, created via support from the Centers for Disease Control and Prevention (CDC):

EMPLOYER CHECKLIST: FORMING BUSINESS AND PUBLIC HEALTH PREPAREDNESS PARTNERSHIPS

This checklist is intended for businesses engaged in improving plans and forming partnerships for emergency preparedness and response. The focus is on terrorism, included as a component of an all-hazards approach to emergency planning and preparation. All-hazards emergency planning enables clear and concise response guidance and customization of plans for the most likely threats.

Checklist guidance regarding partnership with public health agencies is detailed: Each business should also consider developing similar plans and relationships with law enforcement and emergency management agencies.

There are twenty-seven tasks in five checklist categories. Explanations, corresponding resources and referral information for this checklist can be found in the Business Group's Terrorism and Public Health Emergency Preparedness toolkit and online at www.businessgrouphealth.org/prevention/cdc_bioterrorism.cfm. The order of the tasks may vary between businesses depending on current preparedness status.

National Business Group on Health

Planning Tasks 1-8

1 □ Secure support from senior management for improvement and maintenance of emergency preparedness and response capacity.

2 □ Read FEMA's Emergency Management Guide for Business and Industry. Section 1 has a four-step planning process. Section 2 has emergency management considerations.

3 □ Identify and collect all corporate emergency plans, policies, and procedures. Compare with Emergency Management Guide "Threat Assessment" and "Emergency Management Considerations" sections to identify gaps. Establish a planning team, mission, and objectives for a singular all-hazards plan.

4 □ Identify threats to business continuity that are not in current plans. Add threat-specific modules to the all hazards plan. Identify, evaluate and prioritize all natural, man-made, internal and external threats.

5 □ Designate employees responsible for emergency preparedness and response. This includes the planning team and emergency response team. Develop incident management system including specific functional areas (building management, etc.). Inventory internal resources including employee capacity. Set up redundancies in emergency contact system.

6 □ Empower a senior manager with extraordinary decision-making authority for emergency situations that are not covered in the plan. Set up redundancies in decision-making authority.

7 □ Modify and update an all-hazards plan. This includes activation of the emergency response team, immediate scene control and communications.

8 □ Obtain senior management approval of updated plans.

Coordination Tasks 9-14

9 □ Contact local emergency management agency to discuss (911) emergency response communications. Also contact local Poison Control Center and discuss appropriate use of Center resources in an emergency. Determine key contacts and chain of communications.

10 □ Contact nearest FBI Field Office. Discuss emergency response (terrorism) communication and planning. Request sharing of plans. Determine key contacts and chain of communications.

11 □ Contact local emergency management agency. Discuss emergency communications and planning. Request sharing of plans and establish a communication network. Contact state EMA if local organization is limited. Determine key contacts and chain of communications.

12 □ Contact local public health agency. Discuss emergency communications and planning.Request sharing of plans and establish a communication network. Consider contacting state Bioterrorism Coordinator if local organization has limited resources.Determine key contacts and chain of communications.

13 □ Consider contacting key vendors, suppliers and contractors. Discuss and plan for business continuity during and after emergencies. Incorporate into all-hazards plan. Determine key contacts and chain of communications.

14 □ Consider working with business partners and business groups on emergency preparedness and response. Business groups and non-government organizations may be active in emergency preparedness initiatives. Determine key contacts and chain of communications.

Internal Implementation Tasks 15-19

15 □ Disseminate the plan internally as widely as needed. Ensure key individuals read and understand roles. Consider posting on an intranet, adding to policies and procedures manual, including in training schedule of managers.

16 □ Connect employees with appropriate emergency preparedness and response resources, education and training opportunities. Emergency management and public health training available through FEMA and CDC, respectively.

17 □ Add emergency preparedness and response to employee support program schedule. Also, consider adding emergency preparedness and response to health fair activities (e.g. include with employee safety exhibits and activities).

18 □ Identify additional employees interested in community emergency preparedness and response. Support development of teams and team leadership. Consider participation in Citizen Corps and local disaster volunteer organizations.

19 □ Test critical plan components. Activate emergency response team. Run drills on evacuation, shelter-in-place, threat containment, and employee relocation procedures. Consider requesting outside evaluation of plans and tests. Capture lessons learned and incorporate into plans.

External Implementation Tasks 20-24

20 □ Disseminate the plan as needed among business partners, health officials and first responders. Ensure key individuals read and understand roles.

21 □ Test communications links used in response: First responder, FBI, emergency management agency, and pulic health agency. Report a scenario and discuss response issues. Capture lessons learned. Update plans as necessary.

22 □ Request participation in government-led emergency response exercises. Start with local emergency management agency.

23 □ Exercise emergency response and public health specific plans. These include threat detection, biological agent response, chemical agent response and risk communication.

24 □ Request meeting with major insurers and health plans covering employees. Discuss disaster-related business issues, identify extraordinary decision makers, and establish emergency communications. Determine override capabilities and other issues for emergencies.

Evaulation Tasks 25-27

25 □ Ensure the plan includes a regular review and update cycle. Consider annual review if plan is not part of established review cycle.

26 □ Collect and consolidate lessons learned and feedback from external agencies. Update plan as necessary.

27 □ Ensure that each implementation task involving a test of part of the plan includes and evaluation and feedback loop. Keep the plan dynamic. Encourage evaluation and adjustment.

This checklist was produced with the support of the U.S. Centers for Disease Control and Prevention.

The National Business Group on Health, with the support of the Centers for Disease Control and Prevention, produced the above checklist as part of an informative and functional resource for employers entitled "An Employer Toolkit: Terrorism Preparedness & Planning: A Public/Private Partnership." This toolkit provides employers with pertinent and timely information about practical strategies around emergency planning and response, working with Public Health, sharing plans, and coordinating efforts. For more information, please see http://www.businessgrouphealth.org/prevention/et_terrorismpreparedness.cfm.

6.0 HOW TO RESPOND TO A TERRORIST ATTACK

6.1 Internal Corporate response to terrorist attacks

6.1.1 The Challenge

The foundations of response begin during the pre-event stage with awareness, education, and emergency planning. Terrorism shocks the psyche and disrupts the daily routines of its victims through senseless acts of destruction. When terrorists strike, business leaders need to anticipate the effects such an event will have upon their employees.

During terrorist attacks, mass anxiety can result. Employees may display psychosomatic symptoms feelings of dread, breathing difficulties, profuse sweating, tremors, or mood swings. "Worried well" victims can overwhelm local health care systems and deflect treatment from the more seriously injured. Supervisors as well as fellow workers should be capable of recognizing both the overt and subtle warning signs of those affected.

When terrorists strike, business leaders need to anticipate the effects such an event will have upon their employees. Protecting the workforce is priority number one.

6.1.2 Protecting the Workforce

Terrorist events demand decisiveness to offset the ambiguity and chaos of the moment. Protecting the workforce is priority number one. Be prepared to implement emergency actions suitable to the danger faced. Stay attuned to your surroundings, as information about the attack may be incomplete and communication systems unreliable.

Clearly communicate what emergency measures you and your management team will implement following an unexpected event: evacuation, sheltering-in-place, or dismissal. Determine the degree of threat to your facility and the best routes of travel once conditions permit the release of employees. To do this, information sharing arrangements are key.

Remain in contact with law enforcement, medical representatives and public officials. Others within your organization will look to you for direction and guidance. Leaders must remain calm even under the most onerous conditions.

If emergency evacuation is necessary and can be accomplished safely, direct your employees to pre-established rally points. Take roll call and account for any visitors at your site. Ensure building and facility security are deployed and lending assistance. Security must stay in contact with the company leadership in order to execute subsequent decisions or actions. The strength of any evacuation plan hinges on detailed planning and regular rehearsals.

6.2 Responding to Terrorist attacks

6.2.1 Emergency Communications and Information

A good communications plan includes rumor control, especially during rapidly developing situations. Getting accurate and instructive information to employees can help head off confusion, hysteria, and panic. The flow of actionable and timely information to employees should commence as soon as possible and continue well into the recovery period.

Businesses leaders have a responsibility to educate their workforce about potential threats and precautions and protective measures to take. If people know what to do in advance, then subsequent response actions have a much better chance of success.

Business leaders have a responsibility to educate their workforce about potential threats and precautions and protective measures to take.

Internal communication plans should augment public sector information programs. By collaborating with governmental partners during the pre-event stage, employers can inform their workers about current threats and protocols for safeguarding those at risk. Business and industry leaders can also support governmental efforts by offering credible spokespersons to allay pubic concerns, instill confidence in responding agencies, and reinforce appeals for cooperation and compliance.

6.2.2 Aiding Communities: Private Sector Emergency Response

The private sector has a vested interest in protecting the contiguous communities they serve. Furthermore, companies want their workforces and families kept out of harm's way. By teaming with governmental agencies and departments, companies can forge productive public-private partnerships dedicated to information sharing and asset augmentation.

Public-private partnerships improve the overall efficiency and effectiveness of response and recovery efforts. Joint planning and exercising using Department of Homeland Security scenarios are ready-made tools for building public-private sector interoperability and synergy. Identifying and committing private sector assets and key resources during the preparatory phase of emergency management can help offset possible shortfalls anticipated during response. The private sector can lend much needed technical expertise, assets, and materials if public sector agencies are overwhelmed by the sheer magnitude of a catastrophic event.

Business community volunteers specially trained in niche aspects of emergency management become force multipliers when local and state responders are stretched beyond capacity. Commercial facilities can serve as points of distribution during biological events or as collection points for donations following major disasters. The type and level of private sector support will depend upon the nature of the emergency and the scope of mitigation and recovery operations undertaken.

7.0 HOW TO RECOVER FROM A TERRORIST ATTACK

7.1 Damage Assessments / Financial Recovery

If a terrorist attack directly affects your organization, it is imperative to quickly conduct a damage assessment in order to understand the financial aspects of your organization's recovery and remediation efforts. The following damage assessment details should be part of every EP&R:

- Account for all damage-related costs. Establish special job order numbers and charge codes for purchases and repair work.
- Assess the value of damaged property.
- Assess the impact of business interruption associated with recovery.
- Take an inventory of damaged goods. This is usually done with the adjuster, or with the adjuster's salvor if there is any appreciable amount of goods or value. If you release goods to the salvor, obtain a signed inventory stating the quantity and type of goods being removed.
- Restore equipment and property (or obtain a time and cost estimate for restoration of the same). For major repair work, review restoration plans with your insurance adjuster and appropriate government agencies.
- Assess remaining hazards, if any.
- Business recovery and restoration go right to a facility's bottom line: Keeping people employed, the business running, and the community thriving.

Business recovery and restoration go right to a facility's bottom line: Keeping people employed, the business running, and the community thriving.

7.2 Continuity of Operations Plans (COOP)

How quickly your company can get back to business after a terrorist attack or a natural disaster (tornado, hurricane, fire, flood, etc.) often depends on the emergency planning performed in advance. A continuity of operations component of a solid EP&R will improve the likelihood that your company will survive and recover from a terrorist act.

According to the Department of Homeland Security, a continuity of operations plan includes the following steps:

1. Carefully assess how your company functions, both internally and externally, to determine which staff, materials, procedures, and equipment are absolutely necessary to keep the business operating.
   - Review your business process flow chart if one exists.
   - Identify operations critical to survival and recovery. Could the company continue to provide deliverables, products, or services to clients in the event of a terrorist attack? For how long?
   - Include emergency payroll, expedited financial decision-making, and accounting systems to track and document costs in the event of a disaster.
   - Ensure necessary and critical paper and electronic files are frequently backed-up. Are the files stored on-site or off-site? Are critical files, papers, and backed-up data stored in fireproof vaults?
   - Establish procedures for succession of management. Include at least one person who is not at the company headquarters, if possible.
2. Identify your suppliers, shippers, resources, and other businesses you must interact with on a daily basis.
   - Develop professional relationships with more than one company to use in case your primary contractor cannot service your needs. A disaster that shuts down a key supplier can be devastating to your business.
   - Create a contact list for existing critical business contractors and others you plan to use in an emergency. Keep this list with other important documents on file, in your emergency supply kit, and at an off-site location.
3. Plan what you will do if your building, plant or store is not accessible. This type of planning is what is most often referred to as a continuity of operations plan and includes all facets of your business.
   - Consider if you can run the business from a different location.
   - Develop relationships with other companies to use their facilities in case a disaster makes your location unusable.
   - Consider where critical employees would work.
4. Plan for payroll continuity. Does the company have adequate business interruption insurance? Does the company have an adequate line of credit or financial capacity to allow it to continue for a sufficient period of time if the workplace needs to be decontaminated or rebuilt?
5. Decide who should participate in putting together your emergency plan.
   - Include co-workers from all levels in planning and as active members of the emergency management team.
   - Consider a broad cross-section of people from throughout your organization, but focus on those with expertise vital to daily business functions. These will likely include people with technical skills as well as managers and executives.
6. Define crisis management procedures and individual responsibilities in advance.
   - Make sure those involved know what they are supposed to do.
   - Train others in case you need back-up help.
7. Coordinate with others.
   - Meet with other businesses in your building or industrial complex.

A continuity of operations component of a solid EP&R will improve the likelihood that your company will survive and recover from a terrorist act.

- Talk with first responders, emergency managers, community organizations, and utility providers.
- Plan with your suppliers, shippers, and others you regularly do business with.
- Share your plans, encourage other businesses to set in motion their own continuity planning, and offer to help others.

8. Review your emergency plans annually. Just as your business changes over time, so do your preparedness needs. When you hire new employees or when there are changes in how your company functions, you should update your plans and inform your people.
9. Understand the effort behind a complete corporate relocation. Have a location identified should a terrorist attack prohibit corporate operations at your original facility. Ensure that this new location can support the business.

7.3 Post-Incident Employment / Mental Health Issues

Following an event or attack, employees may act anxious, dazed, or incoherent even when not affected directly. Their immediate concern will be for the welfare of their loved ones. However, critical incident stress may manifest itself days, weeks, or possibly months later.

Restoration of mental health following a terrorist event may be a prolonged process. The impact upon mental health may extend well beyond those who directly experienced the disaster, possibly including those who witnessed events via television or other media.

The impact upon mental health may extend well beyond those who directly experienced the disaster, possibly including those who witnessed events via television or other media.

Reaching a “new normal” as rapidly and safely as possible is important for minimizing the debilitating impact of terrorism. Companies, even ones that continue to operate at reduced levels, play a vital role in restoring a sense of normality. Going forward with the World Series in New York City, albeit under extraordinary security, after the 9/11 attacks greatly aided the healing process of New Yorkers.

Employers need to recognize the importance that employees will place upon ensuring the safety of their family members and other loved ones before returning to work. Societal norms have created expectations that health care workers, public safety officials, and other emergency personnel will report for duty, regardless of the level of threat to personal health or safety. But recent surveys of hospital staff and administrators have consistently identified care for family members of staff as the highest priority and the most likely barrier to an effective hospital response. Unless addressed in advance, similar concerns among non-health-care workers could delay their return to the workforce.

Mental health recovery and remediation issues are an important part of an organization’s emergency preparedness & response plans.

8.0 SUMMARY

No company executive likes to think about planning for or responding to a terrorist attack at his or her workplace. But the events of September 11 and the following anthrax attacks served as a wake-up call to American businesses that ignoring such threats and being complacent is not a good business decision.

It is incumbent upon the business community to take steps to develop emergency preparedness and response plans to help ensure that a terrorist attack in the workplace can be effectively handled. In many ways, EP&R development for such attacks is not dramatically different than developing response plans for natural disasters or other crises and may in fact be applicable to the latter. However, issues of hardening the workplace, increasing awareness of potential terrorist threats, training, and interacting with governmental agencies can be specific to this type of planning.

It is incumbent upon the business community to take steps to develop emergency preparedness and response plans to help ensure that a terrorist attack in the work-place can be effectively handled.

When considering plans for and responses to a terrorist event, it is clear that the private sector must work closely with local first responder organizations (emergency management, police, fire, and public health agencies). An important step in a business’ development of an effective EP&R is to build a better understanding of and liaison with the appropriate public health and public safety personnel and to integrate its efforts with those of government. We hope this primer underscores the need for that integration and helps educate executives and others in the business community on how best to prepare for terrorism.

NOTE: In December of 2005, the President of the United States announced an ambitious program requiring all federal, state and local authorities to prepare response plans for pandemic influenza. While pandemic influenza is not a terrorist threat, much of this primer could be applied to a pandemic flu outbreak. This primer includes an Appendix E: Preparing for Pandemic Influenza to assist the business community in this area.

Appendix A — Links to Agencies and Organizations Nationwide

U.S. Department of Homeland Security
Main Info: http://www.dhs.gov
Basic Disaster Preparedness info: http://www.ready.gov

White House Homeland Security Page
http://www.whitehouse.gov/infocus/homeland/index.html
http://www.whitehouse.gov/homeland/contactmap.html

U.S. Department of Defense Homeland Security Page
http://www.defenselink.mil/specials/homeland/

National Institute for Occupational Safety and Health (NIOSH)
Main Info: http://www.cdc.gov/niosh/homepage.html
Building Safety: http://www.cdc.gov/niosh/bldvent/2002-39E.html
Emergency Preparedness for Business: http://www.cdc.gov/niosh/topics/prepared/prepared_contact.html

Centers for Disease Control and Prevention (CDC)
http://www.cdc.gov
http://www.bt.cdc.gov/emcontact/index.asp;
http://www.bt.cdc.gov/links.asp

State Public Health Agencies
http://www.statepublichealth.org

U.S. Army Corps of Engineers protecting buildings and their occupants
http://buildingprotection.sbccom.army.mil/basic/

Federal Emergency Management Agency
http://www.fema.gov

Emergency Management Guide for Business and Industry
http://www.fema.gov/library/bizindex.shtm

U.S. Environmental Protection Agency
http://www.epa.gov
http://www.epa.gov/iaq/largebldgs/baqtoc.html

American Red Cross
Main Info.: http://www.redcross.org
Business and Industry Guide: http://www.redcross.org/services/disaster/beprepared/busi_industry.html

U.S. Postal Service
Mail Handling procedures: http://www.usps.com/news/2001/press/pr01_1010tips.htm

U.S. Department of State
Travel warnings: http://www.travel.state.gov/travel_warnings

Small Business Administration
http://www.ibhs.org/docs/openforbusiness.pdf

Appendix B — Listing of Homeland Security Resources

National Homeland Security Knowledge Base
http://www.nationalhomelandsecurityknowledgebase.com/

Homeland Security Insititute
http://www.homelandsecurity.org/resources

National Terror Alert
http://www.nationalterroralert.com/readyguide/quickreference.htm

Homeland Security Weekly
http://www.homelandsecurityweekly.com/resources.html

National League of Cities
http://www.nlc.org/Resources_for_Cities/index.cfm

Corporation for National and Community Service
http://epicenter.nationalserviceresources.org/index.taf?_function=list&Layout_0_Keywords=homeland%20security

Consumer Guides
http://www.consumer-guides.info/Homeland_Security/Preparedness/index.html

Appendix C — Physical Security Assessment Checklist (Draft)

*** This document is a draft. Questions should be modified or deleted based on the specific nature and requirement of the business being assessed.**

Requirement	Yes	No	N/A	Comment
THREAT ASSESSMENT Are current crime statistics for the area on file (CAP Index study)?				
Is there a history of Outsider criminal acts conducted against the facility?				
Is there a history of Insider criminal acts against the facility?				
Is there a history of workplace violence, by insiders or outsiders? Has the facility ever had a bomb threat, when, how many, any found?				
Is the facility an attractive target to terrorists?				
Are there indicators that similar facilities / locations have been targeted by terrorists or terrorist groups?				
Are detailed building plans for the facility readily available from the operating municipality to any person requesting to view or make copies of such plans?				
Is there a mechanism in place to obtain and act upon feedback from any employees on security issues?				
Have lines of communication been established with local, state, and federal law enforcement?				
Have lines of communication been established with neighboring industrial facilities?				
Is there a site policy/procedure that addresses termination of employees?				
Are photos of terminated employees banned from the premises provided to security / reception staff?				

A complete version of the Physical Security Assessment Checklist can be found at http://www.bens.org/AppendixC_1010507.pdf.

Appendix D — Private Sector Security Measures tied to the DHS Homeland Security Alert System

Security Measures	HSAS Threat Levels				
	[*]L	G	E	H	S
1. Review, test, and refine security plans (e.g., fire, bomb threats, biological threats, suspicious mail, cyber attacks, evacuation, emergency-employee lists for ID card stickers, employee phone lists, and business continuity policies/procedures.)	X	X	X	X	X
2. Regularly train personnel on security plans, HSAS response measures, security standards, and security procedures.	X	X	X	X	X
3. Regularly conduct facility risk and vulnerability assessments, which include possible impact from surrounding facilities. Install security equipment and plan measures required at higher threat levels. Identify critical facilities.	X	X	X	X	X
4. Identify and conduct risk & vulnerability assessments on critical processes and technical systems.	X	X	X	X	X
5. Implement positive I.D. access-control procedures for all people (including visitors and contractors) at critical facilities. Require use of company Photo ID. or government-issued Photo ID. Keep access logs.	X	X	X	X	X
6. Ensure existing security measures such as fencing, locks, camera surveillance, intruder alarms, card-access security systems and lighting are in proper working order.	X	X	X	X	X
7. Develop and implement hardware, software, and communications security for computer-based operational systems.	X	X	X	X	X
8. Establish local, regional, and systemwide emergency threat and warning communication processes, within the company, with law enforcement, and with state and regional industry regulation agencies.	X	X	X	X	X
9. Ensure all emergency-services agencies have directions to your site and phone numbers of critical site personnel. Request periodic patrol checks from police agency serving your facility.	X	X	X	X	X
10. Advise all personnel at each facility to report the presence of unknown suspicious persons, vehicles, mail, and other suspicious activities.	X	X	X	X	X
11. Review and test emergency operations plans with suppliers, contractors, and business affiliates (landowners, building managers of tenant offices, etc.).	X	X	X	X	X
12. Caution personnel not to talk to outsiders concerning their facility or its operations. Coordinate the release of information to the media with the Communications and Security Departments.	X	X	X	X	X
13. Review guard service contract compliance, post orders, training programs, and emergency staffing capabilities.	X	X	X	X	X
14. Make sure security signage is in place at all facilities.	X	X	X	X	X
15. Establish policies on prosecution of criminal offenses against the Company.	X	X	X	X	X
16. Ensure gloves are available for people handling mail and deliveries.	X	X	X	X	X
17. Communicate higher alert level to all personnel.		X	X	X	X
18. Review all operations plans, personnel assignments, and logistical requirements that pertain to implementing higher threat conditions.		X	X	X	X
19. Expedite completion of all outstanding maintenance and capital project work that could affect the security of facilities.		X	X	X	X
20. Communicate higher alert level to all personnel, nearby facilities, and emergency responders			X	X	X
21. Test security and emergency communication procedures to ensure security plans can be mobilized for increased threat level.			X	X	X
22. Encourage community security awareness of suspicious activity.			X	X	X
23. Close and lock gates, except those needed for immediate entry and egress at critical facilities. Install road barriers, if needed.			X	X	X
24. Limit visitation and confirm that every visitor is authorized to be at a critical facility. All unknown visitors should be escorted on critical facilities.			X	X	X
25. Increase frequency of security inspections and patrols within the facility giving special attention to buildings, storage tanks, water intake, gas and electric supply, and telecommunications facilities.			X	X	X
26. Increase frequency of security inspections of unmanned sites and remote sites, including critical ROW.			X	X	X
27. Direct that all personal, company, and contractor vehicles at critical facility sites be secured and parked at a distance from critical areas.			X	X	X
28. Ensure that all telephone, radio, and satellite communication systems are in place and operational.			X	X	X
29. Implement procedures requiring facility maneuvers to periodically provide periodic update status of security measures being implemented.			X	X	X
30. Identify the owners of all vehicles at critical facilities and remove all vehicles whose owners have not been identified.			X	X	X
31. Communicate higher alert level to all personnel.				X	X
32. Confirm the availability of security resources that can assist with 24 x 7 coverage of critical facilities, evaluate assigning guards, especially during nondaylight hours, weekends and holidays, and implement according to plan. Prepare to work at alternate sites or with adjusted workforces.				X	X
33. Assign personnel at critical facilities to assist with security duties. (monitoring personnel entering the facility checking vehicles entering the facility, patrolling the area regularly, and reporting security concerns to facility management).				X	X

[*] Low, Guarded, Elevated, High, and Severe

34. Verify all incoming vehicles and people are authorized. Check, to the extent possible, all vehicles, people, mail, packages, brief cases, etc. entering and leaving the site and placard visiting vehicles indicating they have been checked by security.				X	X
35. Consult local authorities about control of public roads and access points that might make the facility more vulnerable to terrorist attack if they were to remain open.				X	X
36. Advise all personnel to inspect deliveries, packages, mail, etc. and notify the supervisor if there is any concern.				X	X
37. Erect more barriers to control direction of traffic flow and protect the affected facility from an attack by moving heavy company vehicles and installing collision barriers. Implement centralized parking and shuttle-bus service where feasible.				X	X
38. Move automobiles and other nonstationary items at least 30 yards from critical facilities, particularly buildings and sensitive areas, unless doing so would create a safety hazard or impede other security measures in place at the facility. Identify areas where explosive devices could be hidden.				X	X
39. Resurvey the surrounding area to determine if activities near a critical facility (e.g., airports, government buildings, industrial facilities, railroads, other pipelines) could create hazards that could affect the facility.				X	X
40. Secure critical facilities 24 x 7 using either contract or company personnel; ensure that all security personnel have been briefed on policies governing the use of force and pursuit (as appropriate). Restrict access to essential personnel only at critical facilities.				X	X
41. Advise local police agencies that the alert level is at a High Condition (Orange) and advise them of the security measures being employed. Request police agencies to increase the frequency of their patrols of the facility.				X	X
42. Cancel or delay all nonvital facility work conducted by contractors, or have company personnel continuously monitor the contractors' work.				X	X
43. Instruct employees working alone at remote locations or on the ROW to check in periodically.				X	X
44. Practice emergency action plans.				X	X
45. Communicate higher alert level to all personnel.					X
46. Activate emergency response plans for the critical facilities. Redirect personnel to address critical emergency needs.					X
47. Augment security forces to ensure control of the facility and access to the facility and other potential target areas. Establish surveillance points and reporting criteria and procedures.					X
48. Inspect all vehicles entering critical facilities including the cargo areas, undercarriage, glove compartments, and other areas where dangerous items could be concealed.					X
49. Refuse access to people who do not have positive identification or do not have a legitimate need to enter the site.					X
50. Reduce site ingress and egress points to an absolute minimum.					X
51. Increase the frequency of call-ins from remote locations. Employees should not work alone in high-risk remote facilities.					X
52. Guards should continually check the perimeter fence and critical facilities while staying in communication with site personnel via two-way radio.					X
53. Shut down affected facilities and operations in accordance with contingency plans unless there is a compelling reason not to. Reduce staffing at high-risk facilities to lowest possible levels.					X
54. Request assistance from the local police agencies in securing the facility and access.					X
55. Implement business contingency and continuity plans as appropriate.					X
56. Request consistent patrol checks from the police agency serving your facility.					X

Appendix E — Preparing for Pandemic Influenza

What is a Pandemic?

A pandemic is a worldwide outbreak of a disease. An influenza (flu) pandemic occurs when a new flu virus appears or "emerges" in the human population, causes serious illness, and then spreads easily from person to person worldwide.

Pandemics are different from seasonal outbreaks or "epidemics" of the flu:

- ***Seasonal outbreaks*** are caused by subtypes of flu viruses that already exist among people.
- ***Pandemic outbreaks*** are caused by new subtypes or by subtypes that have never circulated among people or have not circulated among people for a long time.

In a typical flu season, 36,000 people die of the flu in the United States, mostly the elderly. Past influenza pandemics have led to much higher levels of illness, death, social disruption, and economic loss.

Flu Pandemics During the 20th Century

During the 20th century, the emergence of new flu virus subtypes caused three pandemics, all of which spread around the world within one year of being detected.

- In 1918-19, the "***Spanish flu***" caused the highest number of known flu deaths. More than 500,000 people died in the United States. Up to 50 million people may have died worldwide. Many people died within the first few days after infection, and others died of complications later. Nearly half of those who died were young, healthy adults. For every 1,000 people who got the Spanish flu, 20 died.
- In 1957-58, "***Asian flu***" caused about 70,000 deaths in the United States. First identified in China in late February 1957, the Asian flu spread to the United States by June 1957.
- In 1968-69, "***Hong Kong flu***" caused about 34,000 deaths in the United States. This virus was first detected in Hong Kong in early 1968 and spread to the United States later that year. For every 1,000 people who got the Hong Kong flu, 5 died.

Both the Asian flu and the Hong Kong flu pandemics were caused by new viruses created when a human flu virus and an avian (bird) flu virus combined. many researchers also now believe the 1918-19 pandemic virus originated from a bird flu virus.

Stages of a Pandemic

The World Health Organization (WHO) has defined six phases of a pandemic:

Interpandemic period (between pandemics)

Phase 1: No new flu virus subtypes have been detected in humans. A flu virus subtype that has caused human infection may be present in animals. If present in animals, the risk of human infection or disease is considered to be low.

Phase 2: No new flu virus subtypes have been detected in humans. However, a circulating animal flu virus subtype poses a substantial risk of human disease.

The difference between phase 1 and phase 2 is based on scientists' judgment of the risk of humans becoming infected by the subtypes that are infecting animals.

Pandemic alert period

Phase 3: Humans have become infected with a new subtype, but there has been no spreading of the virus from person to person.

Phase 4: There has been some human-to-human transmission, but it has been limited to small, highly localized cluster(s), suggesting that the virus is not well adapted to humans.

Phase 5: Human-to-human spread is still localized, but now occurs in larger cluster(s), suggesting that the virus is becoming increasingly better adapted to humans but may not yet be fully transmissible (substantial pandemic risk).

The distinction between phases 3, 4, and 5 is based on scientists' judgment of whether the virus is well-adapted to humans, how quickly it will spread, and how sick people will get when they have the virus.

Pandemic period

Phase 6: Human-to-human spread has increased and is sustained in the general population.

Preparing for the Next Pandemic

Influenza pandemics have historically taken the world by surprise, giving health services little time to prepare for the abrupt increases in cases and deaths that characterize these events and make them so disruptive. Vaccines the most important intervention for reducing morbidity and mortality were available for the 1957 and 1968 pandemic viruses but arrived too late to have an impact. As a result, great social and economic disruption, as well as loss of life, accompanied the three pandemics of the previous century.

The present situation is markedly different because the world has been warned in advance. For some time now, conditions favoring another pandemic have been unfolding in parts of Asia. This advance warning has brought an unprecedented opportunity to prepare for a pandemic and develop ways to mitigate its effects.

While neither the timing nor the severity of the next flu pandemic can be predicted, many scientists believe it is only a matter of time until one occurs. Its effect in the United States could be severe. Modeling studies suggest that, without vaccination or drugs, a "medium level" pandemic could cause:

	U. S.	Georgia
Deaths	89,000 to 207,000	2,600 to 6,200
Hospitalizations	314,000 to 734,000	9,400 to 22,000
Office visits	18 to 42 million	540,000 to 1.26 million
Sick	20 to 47 million	600,000 to 1.4 million

* Up to 15% of the U.S. population would be affected.

A pandemic as severe as the Spanish flu in 1918 1919 could cause:

	U. S.	Georgia
Deaths	About 1.9 million	About 57,000
Hospitalizations	About 8.5 million	About 255,000
Office visits	About 86.6 million	About 2.6 million
Sick	About 93.3 million	About 2.8 million

* 35% of the U.S. population could be affected.

How to Prepare for Pandemic Flu

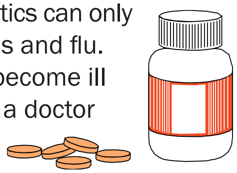
Preparing for pandemic flu involves taking steps to limit, as much as possible, the number of people who get sick and preparing to take care of possibly large numbers of people who do become sick. Preparing for a pandemic is not only the job of public health officials, doctors and hospitals. Individual citizens and community organizations need to prepare as well, for the following reasons:

- A vaccine probably will not be available in the early stages of a pandemic.
- Antiviral medications will be in short supply and may not work if the virus becomes resistant.
- Antibiotics do not work against viruses
- There are some simple self-care activities that can greatly reduce the chances of getting the flu.

A vaccine probably will not be available in the early stages of a pandemic.
When a new vaccine against a flu virus is being developed, scientists around the world work together to select the virus strain that will offer the best protection against that virus, and manufacturers then use the selected strain to develop a vaccine. Once a potential pandemic strain of flu virus is identified, it takes several months before a vaccine will be widely available. If a pandemic occurs, it is expected that the U.S. government will work with many partner groups to make recommendations to guide the early use of any vaccine.

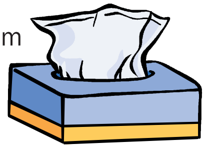
Antiviral medications will be in short supply, and may not work if the virus becomes resistant.
Four different flu antiviral medications (amantadine [Symmetrel]), rimantadine [Flumadine], oseltamivir [Tamiflu], and zanamivir [Relenza]) are approved by the U.S. Food and Drug Administration (FDA) for the treatment and/or prevention of flu. However, sometimes flu virus strains can become resistant to one or more of these drugs, and the drugs may not always work. For example, the avian flu viruses identified in human patients in Asia in 2004 and 2005 have been resistant to amantadine and rimantadine. Monitoring of avian viruses for resistance to flu antiviral medications is continuing.

Antibiotics do not work against viruses
There are two types of germs - bacteria and viruses. Antibiotics can only kill bacteria; they do not kill the viruses which cause colds and flu. If a person is already ill with a cold or flu, they may also become ill with an infection caused by bacteria; when this happens, a doctor may prescribe antibiotics to treat the bacterial infection.



There are simple self-care activities that can greatly reduce the chances of getting the flu.
Because we will not be able to rely on medications, self care will be key to avoiding getting the flu during a pandemic. There are two things that you can do to reduce your chance of getting the flu.

1. ***Keep Away from People Who Have a Cold or Flu.*** Because the viruses that cause these infections are coughed and sneezed into the air you share with other people, it helps to stay away from people who are ill and to avoid enclosed, crowded places if you can. Don't touch other people's used tissues or handkerchiefs. If you have flu, it's better to stay away from work so you don't pass it on to others.



2. ***Wash Your Hands More Often.*** It's very easy to pick up cold and flu germs from things other people have touched - telephones, door handles, or money, for instance - or from shaking hands with someone who is infected. Reduce your risk of catching a cold or flu by washing hands frequently; using warm water and soap removes germs better than a quick rinse under the cold tap. It's also important to avoid touching your eyes, nose, or mouth with your hands - these are all ways that germs can get into your system.

By promoting these measures in our communities, we can slow down the spread of the disease. If we do so, we can reduce the number of people who get sick before a vaccine becomes available.

CDC Business Pandemic Influenza Planning Checklist

Business Pandemic Influenza Planning Checklist

In the event of pandemic influenza, businesses will play a key role in protecting employees' health and safety as well as limiting negative impacts to the economy and society. Planning for pandemic influenza is critical. To assist you in your efforts, the Department of Health and Human Services (HHS) and the Centers for Disease Control and Prevention (CDC) have developed the following checklist for large businesses. It identifies important, specific activities large businesses can do now to prepare, many of which will also help you in other emergencies. Further information can be found at http://www.pandemicflu.gov and http://www.cdc.gov/business.

1.1 Plan for the impact of a pandemic on your business:

Completed	In Progress	Not Started	
□	□	□	Identify a pandemic coordinator and/or team with defined roles and responsibilities for preparedness and response planning. The planning process should include input from labor representatives.
□	□	□	Identify essential employees and other critical inputs (e.g., raw materials, suppliers, sub-contractor services/products, and logistics) required to maintain business operations by location and location during a pandemic.
□	□	□	Train and prepare ancillary workforce (e.g., contractors, employees in other job titles/descriptions, retirees).
□	□	□	Develop and plan for scenarios likely to result in an increase or decrease in demand for your products and/or services during a pandemic (e.g., effect of restriction on mass gatherings, need for hygiene supplies).
□	□	□	Determine potential impact of a pandemic on company business financials using multiple possible scenarios that affect different product lines and/or production sites.
□	□	□	Determine potential impact of a pandemic on business-related domestic and international travel (e.g., quarantines, border closures).

Completed	In Progress	Not Started	
□	□	□	Find up-to-date, reliable pandemic information from community public health, emergency management, and other sources and make sustainable links.
□	□	□	Establish an emergency communications plan and revise periodically. This plan includes identification of key contacts (with back-ups), chain of communications (including suppliers and customers), and processes for tracking and communicating business and employee status.
□	□	□	Implement an exercise/drill to test your plan, and revise periodically.

1.2. Plan for the impact of a pandemic on your employees and customers:

Completed	In Progress	Not Started	
□	□	□	Forecast and allow for employee absences during a pandemic due to factors such as personal illness, family member illness, community containment measures and quarantines, school and/or business closures, and public transportation closures.
□	□	□	Implement guidelines to modify the frequency and type of face-to-face contact (e.g., hand-shaking, seating in meetings, office layout, shared workstations) among employees and between employees and customers (refer to CDC recommendations).
□	□	□	Encourage and track annual influenza vaccination for employees.
□	□	□	Evaluate employee access to and availability of healthcare services during a pandemic, and improve services as needed.
□	□	□	Evaluate employee access to and availability of mental health and social services during a pandemic, including corporate, community, and faith-based resources, and improve services as needed.
□	□	□	Identify employees and key customers with special needs, and incorporate the requirements of such persons into your preparedness plan.

1.3. Establish policies to be implemented during a pandemic:

Completed	In Progress	Not Started	
□	□	□	Establish policies for employee compensation and sick-leave absences unique to a pandemic (e.g., non-punitive, liberal leave), including policies on when a previously ill person is no longer infectious and can return to work after illness.
□	□	□	Establish policies for flexible worksite (e.g., telecommuting) and flexible work hours (e.g., staggered shifts).

Completed	In Progress	Not Started	
□	□	□	Establish policies for preventing influenza spread at the worksite (e.g., promoting respiratory hygiene/cough etiquette, and prompt exclusion of people with influenza symptoms).
□	□	□	Establish policies for employees who have been exposed to pandemic influenza, are suspected to be ill, or become ill at the worksite (e.g., infection control response, immediate mandatory sick leave).
□	□	□	Establish policies for restricting travel to affected geographic areas (consider both domestic and international sites), evacuating employees working in or near an affected area when an outbreak begins, and guidance for employees returning from affected areas (refer to CDC travel recommendations).
□	□	□	Set up authorities, triggers, and procedures for activating and terminating the company's response plan, altering business operations (e.g., shutting down operations in affected areas), and transferring business knowledge to key employees.

1.4. Allocate resources to protect your employees and customers during a pandemic:

Completed	In Progress	Not Started	
□	□	□	Provide sufficient and accessible infection control supplies (e.g., hand hygiene products, tissues and receptacles for their disposal) in all business locations.
□	□	□	Enhance communications and information technology infrastructures as needed to support employee telecommuting and remote customer access.
□	□	□	Ensure availability of medical consultation and advice for emergency response.

1.5. Communicate to and educate your employees:

Completed	In Progress	Not Started	
□	□	□	Develop and disseminate programs and materials covering pandemic fundamentals (e.g., signs and symptoms of influenza, modes of transmission), personal and family protection and response strategies (e.g., hand hygiene, coughing/sneezing etiquette, contingency plans).
□	□	□	Anticipate employee fear and anxiety, rumors and misinformation, and plan communications accordingly.
□	□	□	Ensure that communications are culturally and linguistically appropriate.
□	□	□	Disseminate information to employees about your pandemic preparedness and response plan.

Completed	In Progress	Not Started	
□	□	□	Provide information for the at-home care of ill employees and family members.
□	□	□	Develop platforms (e.g., hotlines, dedicated websites) for communicating pandemic status and actions to employees, vendors, suppliers, and customers inside and outside the worksite in a consistent and timely way, including redundancies in the emergency contact system.
□	□	□	Identify community sources for timely and accurate pandemic information (domestic and international and resources for obtaining counter-measures ([vaccines and antivirals]).

1.6. Coordinate with external organizations and help your community:

Completed	In Progress	Not Started	
□	□	□	Collaborate with insurers, health plans, and major local healthcare facilities to share your pandemic plans and understand their capabilities and plans.
□	□	□	Collaborate with federal, state, and local public health agencies and/or emergency responders to participate in their planning processes, share your pandemic plans, and understand their capabilities and plans.
□	□	□	Communicate with local and/or state public health agencies and/or emergency responders about the assets and/or services your business could contribute to the community.
□	□	□	Share best practices with other businesses in your communities, chambers of commerce, and associations to improve community response efforts.

Acknowledgements

This document would not have been possible without the significant effort of the “Getting Ready” Committee of the BENS Metro Atlanta Region. Thanks are also due to the support, encouragement, and review provided by numerous professionals in the Georgia Division of Public Health.

Business Executives for National Security

For 25 years, Business Executives for National Security has served as the primary channel through which senior executives can help build a more secure America.

In 1982 business executive and entrepreneur Stanley A. Weiss founded the organization around the simple notion that America’s security is everybody’s business and that business leaders have a particularly important contribution to make. Today our members focus on developing new tools to combat new security threats that cannot be deterred or negotiated away and finding new resources to reshape and rebuild our military forces for the 21st Century.

Business and government must cooperate if we are to protect the American homeland against cyber attack, track terrorists’ financial assets, improve intelligence capabilities, and prepare communities to meet a host of new security responsibilities. And the Defense Department must follow the lead of American business to take full advantage of information technology, outsourcing, and privatization to cut the cost of bureaucracy and overhead and invest the savings in our men and women in uniform.

Now more than ever, national security is everybody’s business. Business Executives for National Security proudly helping to secure America’s future.

Business Executives for National Security
1717 Pennsylvania Avenue, NW, Suite 350, Washington, DC 20006-4603
p (202) 296-2125 - f (202) 296-2490 http://www.bens.org

BENS Metro Atlanta Region
191 Peachtree Street, NE, Suite 1500, Atlanta, GA 30303-1924
(404) 220-1268 Phone - (404) 220-1263 Fax
bensatl@bens.org