Mountain Plains Journal of Business and Technology

Volume 4 Article 2

Date Published: 10-1-2003

Organizational Preparation for Terrorist Attack

Alan Wallace
Mesa State College

Vernon Harper
U.S. Army South

Recommended Citation

Wallace, A., & Harper, V. (2003). Organizational Preparation for Terrorist Attack. *Mountain Plains Journal of Business and Technology, 4*(1). Retrieved from https://openspaces.unk.edu/mpjbt/vol4/iss1/2

ORGANIZATIONAL PREPARATION FOR TERRORIST ATTACK

ALAN WALLACE
ASSOCIATE PROFESSOR
MESA STATE COLLEGE

VERNON HARPER
FORMER SPECIALIST IN COUNTER TERRORISM
U.S. ARMY SOUTH

ABSTRACT

In the event of a terrorist attack causing mass casualties or nuclear, biological, or chemical contamination, emergency responders easily can be overwhelmed by demands for their services. Advance planning by organizations with the advice of emergency responders to safeguard people from becoming victims, to care for victims before emergency responders arrive, and to render assistance to emergency responders once they arrive is critical to mitigating damage.

I. INTRODUCTION

During the morning of September 11, 2001, two long-range commercial jet aircraft, piloted by hijackers, intentionally crashed into the World Trade Center in New York City, a third hijacked jet intentionally crashed into the Pentagon in Washington, and a fourth hijacked jet crashed into a field after passengers heard on cell phones about the fate of the other three hijacked jets and overpowered the hijackers. It has been hard for many Americans to come to grips with hopes for our destruction coming from enemies who make no distinction between politicians, the military, and ordinary citizens. Despite the U.S. military campaign in Afghanistan to rout the al Qaeda terrorist organization responsible for the events of September 11, 2001, many al Qaeda members eluded capture and are thought by intelligence agencies to remain in cells throughout the world awaiting orders to act. Al Qaeda may have recruited new members impressed by their success at bringing destruction to America and may have formed alliances with other terrorist organizations with ideological motives and technological capabilities to commit future acts of terrorism within the United States (Johnston, et al., 2002).

After September 11, President Bush created a new agency of Homeland

Security to protect the nation from terrorist attacks. However, the nation is so vast, its population so large, and potential targets so many that government security agencies and emergency responders currently cannot be counted upon to have all of the resources in place when and where they are needed to meet every conceivable contingency (National Commission on Terrorism, 2001). According to Vice President Cheney, it is not a question of if we will have another terrorist attack of such monstrous magnitude, but when.

Although the enormity of the havoc brought to America by foreign terrorists has heightened awareness of the need for organizations to prepare for terrorism, domestic terrorism is also a threat. Timothy McVey was convicted of killing 168 people in the bombing of the Murrah Federal Building in Oklahoma City in 1995. Theodore Kaczynski was arrested in 1996 and charged with mailing bombs on 15 separate occasions to the places of work and the homes of business executives and professors (Associated Press, 1998). Eric Rudolph was arrested in 2003 and accused of detonating bombs at the Atlanta Olympics, two abortion clinics, and a nightclub (Schuster, 2003).

Terrorists attempt to kill, injure, or cause financial losses to targeted victims, and also, they often kill, injure, or cause financial losses to other persons with little or no concern for collateral damage. Terrorists spread fear throughout society. Ways for organizations to alleviate the fear are to understand the weapons and methods used by terrorists, and then to take actions to minimize opportunities for terrorists to strike and to plan, equip, and train personnel to mitigate damage if a terrorist incident occurs.

II. WEAPONS AND METHODS OF TERRORISTS

1. ATTACKS ON DATA NETWORKS

Kevin Mitnick, who has been called a "computer terrorist" by the Department of Justice, was apprehended in 1996 for hacking into the computer networks of Motorola, Nokia, Fujitsu, Novell, NEC, Sun Microsystems, Colorado SuperNet, Netcom On-Line Services, and University of Southern California to steal proprietary software, prevent authorized users from accessing information stored in their accounts, and to run computer "hacking" programs that altered or replaced existing programs (United States District Court, 1996). In February 2000, other computer hackers working in concert shut down the operations of CNN, Yahoo!, eBay, and Amazon.com. Hackers are writing new code all the time to spread viruses through the Internet that attack unprotected computers and overcome anti-virus software to delete files, alter files, or cause systems to crash.

In 2000, the Computer Security Institute conducted a survey of large corporations and government agencies. The survey reported that 90% of respondents had security breaches within the past 12 months; 70% experienced serious breaches such as theft of proprietary information, financial fraud, and sabotage of data networks; 74% acknowledged financial losses; and 273 respondents were able to quantify their losses at $265,589,940 for the past 12 months (Maniscalco & Christen, 2002). In 2001, the executive director of Internet Security Alliance, stated at a House of Representatives hearing that four Internet worm attacks alone, including "Code Red" and "Nimda", cost companies more than $10 billion in systems repairs and lost productivity, and Carnegie Mellon University estimated that the number of security breaches of computer networks more than doubled from 2000 to exceed 40,000 in 2001 (Verton, 2001).

Hackers pioneered techniques that the National Security Agency reports groups hostile to the United States have developed into offensive information warfare capabilities (Minihan, 1998). The Rand Corporation reports that the United States and its allies are "vulnerable to information warfare attacks on their core infrastructures" (Molander, 1996). The Defense Intelligence Agency explained the threat more fully:

> Transnational Infrastructure Warfare involves attacking a nation's or sub-national entity's key industries and utilities; to include telecommunications, banking and finance, transportation, water, government operations, emergency services, energy and power, and manufacturing. These industries normally have key linkages and interdependencies, which could significantly increase the impact of an attack on a single component. Threats to critical infrastructure include those from nation-states, state-sponsored sub-national groups, international and domestic terrorists, criminal elements, computer hackers, and insiders. (Hughes, 1998)

2. ATTACKS USING TACTICAL VIOLENCE

Tactical violence is "the predetermined use of maximum violence in order to achieve one's criminal goals, regardless of victim cooperation, level of environmental threat to the perpetrator, or the need to evade law enforcement or capture" and involves "predatory control of the immediate criminal environment through the creation of chaos and the infliction of terror, trauma, and death on presenting targets" (Maniscalco & Christen, 2002). Tactical violence includes the use of military weapons such as automatic weapons, rocket propelled grenades, hand grenades, mines, and mortars.

The Black September group, Palestine Liberation Organization, Islamic Jihad, Hezbollah, Hamas, and al Qaeda have repeatedly used tactical violence relying on military weapons and improvised high-explosive devices. Some of their massacres include 11 Israeli athletes at the Munich Olympics in 1972; 26 tourists in Israel during 1978; 63 people in the U.S. Embassy and 241 U.S. Marines in their barracks in Beirut, and 111 people on a jet in 1983; 23 more people in the U.S. Embassy in Beirut and 18 U.S. Air Force personnel on their base in Spain in 1984; 58 passengers on a jet and 20 persons at U.S. and Israeli flight check-in desks at the Rome and Vienna airports in 1985; 259 passengers on Pan Am Flight 103 and 11 on the ground in Lockerbie, Scotland in 1988; 19 military personnel in Khobar Towers in Saudi Arabia in 1996; 301 persons in the U.S. Embassies in Kenya and Tanzania that were bombed simultaneously in 1998; 17 sailors on the U.S. Cole in Yemen in 2000; and some 3000 people in the attacks on both the World Trade Center and Pentagon in 2001 (Miller & File, 2001).

3. ATTACKS USING CHEMICALS

One chemical threat is from the release of chemical warfare agents formulated to kill or injure. The other chemical threat is from attacks on chemical plants, chemical storage facilities, and pipelines that spread toxic vapors and droplets of toxic chemicals.

Chemical warfare agents include nerve agents such as sarin, phosgene, and chlorine gas that quickly cause death and blistering agents such as mustard. Simple sprayers and spills can be used to disperse chemical warfare agents. In 1995, members of the Japanese Aum Shinrikyo cult went into a Tokyo subway station and punctured plastic bags of liquid sarin, which evaporated causing the death of 12 people and over 5,500 injuries (Murakami, 1998). Placing a chemical warfare agent in an air circulation system can quickly contaminate entire buildings.

Nerve agents block the activity of an enzyme, which regulates organs and glands in the body, resulting in dangerous over-stimulation. Within seconds of inhalation symptoms appear including reddened watery eyes, small pupils, blurred vision, headache, nausea, vomiting, runny nose, increased salivation, and shortness of breath. If the concentration of vapor is high, consciousness is lost, seizures begin, breathing stops, and death occurs within 5 to 10 minutes. With a liquid droplet on the skin, usually consciousness will be suddenly lost within 30 minutes, breathing ceases, and paralysis and death follow, without any preliminary symptoms (Maniscalco & Christen, 2002).

The second type of threat is from explosions at chemical plants, chemical storage facilities, and in chemical transport equipment that spread vapors and droplets of toxic chemicals. The U.S. Environmental Protection Agency requires approximately 15,000 facilities that produce or store toxic chemicals to report what could happen in a "worst-case scenario" if wind conditions carried toxic vapors and droplets to surrounding areas. In a "worst-case scenario" at over 2,000 facilities, more than 100,000 people could be exposed to toxic chemicals from an explosion (Begley, 2001a).

4. ATTACKS USING BIOLOGICAL AGENTS

Biological threats involve agents which kill and agents that incapacitate people for a period of time. Lethal agents include anthrax and plague, which can spread to others through contact with lesions and secretions. A feature of these live bacteriological warfare agents is an incubation period of several days prior to the onset of symptoms of illness that rapidly lead to death in most cases if not medically treated. In the case of anthrax, treatment is usually not effective unless it begins before symptoms are present. In 1993, Aum Shinrikyo cultured anthrax and sprayed it from the roof of a building in Tokyo (Terrorism Files, 2002). In October 2001, anthrax was mailed within the U.S. to a publishing company, members of Congress, and a television network. A few deaths resulted, and hundreds of people who might have been exposed were prescribed Cipro to fight anthrax. Buildings were shut down for weeks for decontamination. The U.S. Office of Technology Assessment has estimated that a single small plane flying over Washington, D.C. spreading 220 pounds of anthrax spores could kill between 1 and 3 million people and make the city uninhabitable for years (Stephenson, 1996).

Neurotoxins are another class of lethal biological warfare agents. Clostridium is a family of microorganisms that secretes toxins that cause muscle paralysis, respiratory failure, spasms, convulsions, tissues to die and decay, blood vessels to leak, and liver damage. Ricin is produced from castor bean seeds and causes blood vessels to collapse. Some marine animals and amphibians produce tetrodotoxins that cause paralysis and respiratory failure. Some fungi produce trichothecene mycotoxins that inhibit protein and DNA synthesis and destroy cell membranes. The onset of effects is quick, ranging from minutes to a few hours, and death may occur within a few minutes or days, depending on the neurotoxin and the exposure (Maniscalco & Christen, 2002). In 1984, a Paris Police raid on a German Red Army Faction apartment discovered documentation for producing biological warfare agents and a bathtub filled with flasks containing clostridium botulinum (Maniscalco & Christen, 2002). In 1993, Aum Shinrikyo cultured clostridium botulinum and sprayed it around Japanese national legislative buildings (Crime Library, 2002). Also, in January 2003, seven North Africans suspected to be members of al Qaeda were arrested for producing ricin in their London apartment (BBC, 2003a), and in March vials of ricin were found in a storage locker at a Paris train station (BBC, 2003b).

Drinking water systems are especially vulnerable to biological warfare agents. In 1993, 400 thousand people became ill in Milwaukee, Wisconsin and over 50 died when cryptosporidium passed undetected through drinking water treatment plants. Municipal water systems use chlorine to kill e. coli, salmonella, and other common microorganisms, but typically do not test for botulinum toxin, or cryptosporidium that can be killed with ozone, and anthrax spores that can be trapped with filters. (Begley, 2001b)

Non-lethal biological agents include staphylococcal enterotoxins, a common source of food poisoning, and vomiting agents that are easy to spread through food and act quickly to cause nausea, vomiting, and diarrhea. To influence an election outcome, the Bagwan Sri Rajneesh sect spread salmonella on salad bars in four restaurants in The Dalles, Oregon in 1984, causing 750 people to become too sick to vote (Maniscalco & Christen, 2002)

5. ATTACKS USING NUCLEAR AGENTS

One nuclear terrorism threat is from weapons designed to cause radiation sickness and death. Nuclear materials and nuclear weapons stored in the former Soviet Union have not been adequately safeguarded, and former Soviet military officers have been weapons suppliers to al Qaeda, Abu Sayyaf in the Philippines, and other terrorist groups (Farah, 2002). The other threat is from attacks on nuclear plants, nuclear waste storage facilities, and transportation equipment carrying nuclear fuel or waste. An explosion at any one of 103 active private nuclear power plants in the U.S. or their waste storage facilities where 45,000 tons of radioactive spent fuel rods are stored could result in mass casualties (Magnusson, et al., 2001).

Al Qaeda documents, found after the U.S. invasion of Afghanistan, revealed that al Qaeda had a design for a nuclear weapon requiring plutonium, a design for a "dirty bomb" which could use discarded nuclear power plant fuel rods and explosives to disperse radioactive debris over large areas leaving them uninhabitable, and may have been helped by two Pakistani nuclear scientists who helped Pakistan to develop nuclear weapons (Boettcher & Arnesen, 2002).

Nuclear weapons and "dirty bombs", which use explosives to spread radioactive materials over a wide area, present threats to health from two sources, detonation and radioactive decay of atoms. If regular explosives cause detonation, those near the blast site will be threatened from shock waves and debris traveling at high velocity. If a nuclear chain reaction causes detonation, they will also be threatened by intense gamma radiation in the area of the blast site. Gamma rays can strip electrons from atoms in body tissues. Radioactive fallout is a health threat in nuclear chain reactions and "dirty bombs" to both those near the blast site and those downwind of the source of radiation. Fallout consists of dust particles containing lethal radioactive isotopes that continually decay and emit gamma rays. Inhalation or ingestion of radioactive particles can result in damage that may manifest itself within hours, days, weeks, or years. Acute exposure may cause death, destruction of bone marrow, and incapacitation of the digestive and nervous systems. Other effects include sterility, birth defects in unborn children, and cancer. Preventing inhalation, ingestion, and quick decontamination of the skin if exposed to fallout are critical to minimize health threats (Maniscalco & Christen, 2002).

III. PROTECTING AGAINST TERRORIST ATTACKS AND MITIGATING DAMAGE

Terrorists typically look for a weakness or unsecured point of entry that can be exploited. Then they attempt to create an incident of such magnitude that resources available to respond are overwhelmed. There are five steps to be taken to protect against terrorist attacks and to mitigate damage. They are awareness, planning, equipping, securing, and training.

1. AWARENESS

The first step in defending against terrorism is to perform a security audit to identify potential threats and weaknesses in security. If managers have not had comprehensive training in security, security consultants should be involved. Police, fire, and emergency medical services should be involved in the security audit. The security audit team should consist of people who collectively are knowledgeable about all conceivable threats and safeguards.

The World Trade Center and Pentagon, symbols of American power and nerve centers, were targets of terrorists. Any organization that is a symbol of American power, nerve center, or in proximity of critical political, economic, transportation, or communications infrastructure is more likely to be at risk.

Nuclear power plants, chemical plants, refineries, chemical and fuel storage facilities, as well as pipelines and transportation equipment that transport nuclear materials and chemicals are potential terrorist targets because of the mass casualties that could be caused to those in the vicinity and downwind. Public water supply systems are typically unsecured and easy targets for distributing deadly toxins. Building ventilation systems can be used to quickly spread biological, chemical, or radiological agents.

Data networks can be hacked to shut down the power grid, telecommunications, 911 emergency system, or to steal funds to finance terrorism. Organizations with enormous computing and data transmission capacity are tempting targets for hackers who want to spread computer viruses that overwhelm the Internet. Organizations holding financial assets in digital form and confidential credit information are tempting targets for hackers who delete data security programs to allow undetected system entry and theft.

Climate is another factor to consider in threat assessment. In a desert, biological agents are unlikely to cause mass casualties due to the difficulty the agent will have surviving in a low humidity environment outside of living hosts. In humid, forested locations, biological agents can survive outside of living hosts and proliferate quickly over large areas. In a desert, chemical agents would be likely to cause mass casualties over wide areas, while in forested locations the tree canopy would provide some protection to those on the ground level. Prevailing winds and terrain are another factor to consider. Are you downwind of any likely targets? If you live in a valley, dust would tend to collect there raising the risk of exposure to fallout.

A series of questions should be answered about security weaknesses. A partial list follows:

- Is critical electronic data secure from tampering and archived at safe remote locations?
- Are there areas within your facilities where only authorized personnel should be allowed?
- Are restricted areas secured with locks, alarms, surveillance cameras, and or guards?

- Have background checks been done on persons authorized to enter restricted areas?
- Is non-forgeable or non-transferable identification used to verify authorized access?

2. PLANNING

Predicting where, when, and how a terrorist attack will occur is impossible. The best defense to minimize damage from terrorism is to assume that terrorism will occur, to prepare for it, and to develop contingency plans for what would be done by whom in the event of an assortment of possible disasters identified through threat and security system vulnerability assessments. Ultimately, organizational plans must be linked to community plans to minimize damage. But realistically, there are many varieties of terrorist threats that would quickly overwhelm community resources for disaster response. Organizations should prepare to respond to terrorist events in which professional emergency response units are delayed for extended periods of time because of mass casualties or become secondary targets of a terrorist attack and are incapacitated.

Planning should be executed on a need-to-know basis. Explaining the security system and how it works to anyone who wants to know makes it easier for a terrorist to find out about the security system and to evade it. People involved in disaster planning should be advised of the need for confidentiality. Disaster preparedness administrators will need to watch for information leaks and to monitor security systems and equipment for tampering and proper functioning.

Off-site backup storage of data and backup equipment to keep data networks operating might be a part of the plan, depending on how crucial data files and data networks are to the organization and the community. Surveillance systems, lockdown systems, and highly trained security guards with personal protective equipment such as soft body armor, respiratory protection devices, and chemical protective clothing might be a part of the plan, depending on threat assessment. Parts of the plan might include installing monitors for nuclear, biological, or chemical contamination linked to kill switches that shut down a building’s ventilation system as soon as a contaminant is detected; maintaining a stock of filters to trap contaminants and training maintenance personnel to quickly install filters in ventilation systems to restore a safe air supply; and monitoring the health of all people on site for symptoms linked to known contaminants.

Other parts of the plan might include training a security team to stock and issue supplies such as masks to people who could be exposed to biological, chemical, or nuclear contaminants. Another part of the plan might include preparing to conduct mass decontamination. If so, tent-like showers with privacy to convince potential victims to undergo voluntary decontamination, bleach, soap, clean clothes, and contaminated wastewater storage containers need to be stocked in advance.

Being prepared to quarantine large numbers of people can be critical to containing infections from biological agents, as recently seen in the sudden outbreaks of SARS (Sudden Acute Respiratory Syndrome) in China and Toronto, Canada. Biological agents such as SARS reproduce themselves quickly in the bodies of those contaminated, easily spread from those who have been contaminated to infect others, and quickly mutate into new strains to re-infect those starting to recover from the initial strain. Initial health symptoms from many bacteriological agents include fever, fatigue, and mild chest discomfort, not unlike a cold or flu. If large numbers of people in an office, school, or other location suddenly report such symptoms, emergency medical personnel should be alerted. Building areas and exposed individuals may need to be quarantined for observation. Movements of individuals within the organization who are suspected of possible exposure may need to be restricted or traced. Entry by individuals outside the organization suspected of possible exposure may also need to be restricted.

3. EQUIPPING

Effective planning should produce a list of equipment and supplies to be installed on-site for use by authorized personnel within the organization prior to the arrival of emergency response professionals. This equipment must be kept near authorized personnel for easy issue in emergencies. Plans might also include supplies and equipment to be cached for emergency response professionals to draw from once they arrive. Access to this equipment must be restricted to emergency response professionals.

Communication equipment to contact emergency response professionals and to convey instructions to employees and other persons on the premises is essential for all organizations. It should not be assumed that telephones will work, that electricity will be available, or that people will not panic in the absence of quick information about the nature of the situation and clear authoritative directives of what to do coming from credible sources. Each organization needs to designate in advance a temporary incident commander within the organization and alternates, who will oversee emergency communications prior to professional emergency units assigning their own incident commander. The temporary incident commander should be equipped with a battery-operated two-way radio to communicate with police, fire, and medical emergency responders if telephones fail to work. Instructions from emergency responders or the temporary incident commander will need to be passed through internal personnel designated in advance as disaster wardens to alert all persons in their work areas of the emergency and to lead them to safety or shelter. Depending on how facilities are configured, disaster wardens in remote buildings or on different floors may need also to be equipped with battery operated two-way radios for communicating with the incident commander, bullhorns for passing instructions along to those they are leading, and kits containing flash lights, first aid supplies, barrier tape to close off areas evacuated, and writing materials for taking note of who is safe, who is injured with what injuries, and who is unaccounted for to report to emergency responders involved in medical and search and rescue operations.

First aid equipment for properly trained and certified first aid and cardiopulmonary resuscitation (CPR) providers is also a consideration. Red Cross certified first aid and CPR providers are forbidden from going beyond their skill levels; thus, first aid kits for them can be rather simple and inexpensive. However, Red Cross does certify volunteers in the use of an Automatic External Defibrillator (AED), which may cost several thousand dollars. CPR rarely restarts a heart but does circulate blood to vital organs and the brain to keep them alive prior to the arrival of an AED. Every minute that passes when a heart has stopped beating increases the likelihood of death by 10 percent, and that is why quick use of an AED on-site, followed by advanced cardiac support in a hospital is necessary to increase likelihood of recovery in the cardiac chain of survival (Red Cross, 2001). Heart attacks could result from acts of terrorism, but also commonly result from heart disease and accidents; thus, an AED is an item of equipment organizations should consider having on their premises along with personnel certified to use an AED.

Determination of what other equipment to stock should be based on threat assessment and the level of training of personnel within the organization to use the equipment. If an organization is located near a nuclear, chemical, or biological facility, waste disposal site, or on a regular route for transferring such materials, then a Geiger counter or chemical “sniffer” might be included in the equipment list. They cost a few hundred dollars each. Decontamination showers that can properly contain contaminated wastewater, bags to seal airtight personal valuables such as wallets and purses for retrieval later after decontamination, bags to seal contaminated clothing for proper disposal, bleach, soap, and fresh clothing or inexpensive Tyvek suits should also be considered. In gross decontamination all clothing is removed and sealed in a trash bag so it doesn't contaminate anything else. This step alone is estimated to remove 70 to 95 percent of contamination. Then the body is washed with water for one minute under a shower or water hose. In secondary decontamination the body is washed vigorously with a 0.5 percent solution of sodium hypochlorite, which removes exposed surface skin cells along with fallout particles, chemicals, and or biological agents. With certain biological agents, the skin may need to be in contact with a 0.5 percent solution of sodium hypochlorite for more than 10 minutes to be effective. The solution can be prepared by mixing 10 parts water with 1-part undiluted household bleach. Then the body is rinsed thoroughly with water. In the third stage, definitive decontamination, the body is washed thoroughly with soap and water, rinsed thoroughly with water, dried, and clean clothes are put on. (Maniscalco & Christen, 2002)

If tactical violence is believed to be a likely threat to an organization, perhaps because it is within or near a center of political power, is a symbol of power that terrorists would like to destroy, is a repository of financial wealth that could be robbed to finance terrorism, or provides important infrastructure to society, then equipping a professional security force and installing restricted area access identification systems, intruder detection alarm systems, surveillance cameras, and systems to automatically alert emergency response agencies to provide back-up for internal security personnel might be on the equipment list. Soft body armor, self-contained breathing apparatus, and chemical protective clothing might be items to consider for internal security personnel.

Depending on the threat assessment, supplies such as atropine, airways, and other items required in large quantities to treat mass casualties might be considered for caching on-site. Organizations such as airport authorities, sports arenas, convention centers where likely targets of terrorists such as political leaders are in attendance, and organizations near biological and chemical weapons storage and disposal sites in various states might consider caching such supplies. However, they must be secured to ensure access only by trained medical professionals after they arrive on the scene.

Other equipment considerations might include installing direct communications links to emergency responders perhaps triggered by monitoring equipment and installing emergency power backup systems.

Organizations with electrical equipment that provides life support and valuable assets that could be destroyed without precise climate control should certainly include back-up power systems on their equipment lists.

4. SECURING

The first element in securing is to reduce vulnerabilities to unauthorized access to data networks, ventilation systems, critical utility conduits, connections to external utility providers and shutoffs, hazardous materials stored on the premises, security systems, emergency supply caches, and any other equipment and materials that might be of particular interest to terrorists. All of the above should be located on facility blueprints, inventoried, and secured in locked and restricted areas. Access to facility blueprints showing locations of the above, access to inventories reporting detailed descriptions and quantities of items, and access to pass codes and keys should be carefully restricted to personnel who have a need to have them.

The second element in securing is vigilance to detect attempts of unauthorized entry and tampering. Vulnerable networks, systems, equipment, and materials will need to be checked regularly to ensure their integrity, and records should be kept to ensure that tampering or pilferage are detected. Entrusting vigilance over a particular system, equipment, or material solely to one individual may result in poor record keeping and loss of information if that person leaves the organization. Security teams should be created and trained to maintain vigilance over designated systems, equipment, and materials. Personnel who maintain data networks, personnel knowledgeable about ventilation and utility systems in facilities services, and personnel with hazardous material training should be members of teams maintaining security over vulnerabilities that pertain to their areas of expertise.

The third element in securing is forming an incident command team to coordinate response to an incident. The command team should be composed of key officers in the organization who control security, expenditures, logistics, facilities services, and human resources. The command team should strive to develop a seamless interface with police, fire, and emergency medical services as well as entering into mutual assistance agreements with other nearby organizations for emergency supplies, shelter, transportation, and other assistance as needed. The command team, in coordination with professional emergency services, may order areas to be cleared of people and barricaded, and may designate shelter or assembly areas where persons who were on the premises are to report or be transported to be accounted for and assisted. A fairly large team of emergency wardens may be necessary to check presumably still safe areas for occupants, notify occupants of the emergency instructions, lead them to safety, and to account for them and refer them to any further assistance they may need. The command team may also order areas to be cleared of organization personnel and vehicles and restricted for the exclusive use of incoming emergency service vehicles, personnel, and supplies. The command team may direct facilities services and hazardous material personnel to assist in search and rescue operations by providing fire department personnel with facility blueprints with locations of utility shutoffs and hazardous materials. The command team may assist emergency professionals in commandeering areas for victim medical triage, a temporary morgue, and police crime scene management. The command team may also assist emergency services by ordering that support teams put up signs and barricades and post sentinels around the facilities to direct media to a location set up for an official spokesperson of the incident commander, and to prevent media, good Samaritans, curious bystanders, employees, customers, and potential looters from entering the premises.

5. TRAINING

Training should begin with the command team. The command team needs to become aware of potential threats, prevention, and responses necessary to mitigate damage from incidents. Unless members of the command team already have training from prior careers in emergency response agencies, the initial orientation and education of the command team should come from local emergency response agencies and municipal or country emergency managers.

Learning by doing is the next part of training for the command team and begins with planning. The ***Emergency Management Guide for Business & Industry*** published by the Federal Emergency Management Agency (FEMA) in 2001 provides a detailed framework for the command team to develop an emergency response plan that fits the organization they command. An outline of planning items is presented in Appendix 1. As planning items are delegated to specific members of the command team, it should become clearer what types of information needs to be collected, and the material and personnel needed to implement the plan.

The next step in training recommended by FEMA is for the command team to gather in a conference room to conduct emergency scenario exercises during which each member of the team explains the actions that he or she would take in a specific type of emergency. The purpose of these exercises is to reveal omissions in the organization's emergency response plan, areas of overlapping responsibilities and confusion of command team members, and confusion of command team members in how the organization and emergency services will coordinate actions. The command team will need to eliminate gaps in the emergency response plan, establish protocols for decision-making and how to implement decisions among command team members, and come to a mutual understanding with emergency response services regarding the proper actions of the command team prior to and after the arrival of emergency response services.

Once command team members fully understand the scope of what they are to do prior to and after arrival of emergency response services, support teams of personnel will need to be formed to implement each element of the emergency response plan. Support teams should include most or all of the following: security teams, facilities services teams, emergency warden teams to lead people to safe assembly points or shelter, logistics teams to arrange for emergency supplies and transportation, media teams to deal with the press, human resource teams to deal with inquiries from relatives and referrals to services, and recovery teams for salvage and continuing operations elsewhere. Each of these teams will need to receive orientation training and education in the organization's emergency response plan.

The next step in recommended training by FEMA is a walk-through drill involving a representative of each emergency service, the command team, and support teams. Ideally, this training would be conducted during non-business hours when other persons are not on the premises. Similar to the scenario exercises for the command team, this drill is intended to reveal areas of omission, overlap, and confusion among emergency services, the command team, and support teams, which should be remedied prior to involving all personnel. After a walk-through drill and remedying deficiencies, FEMA recommends evacuation and shelter drills involving all employees walking routes to collection points or shelters, accounting for persons, and identifying missing persons.

Finally, to test preparedness for the real thing, the organization may conduct a full-scale exercise simulating an emergency with individuals play-acting victims and involving emergency service commanders, the organization command team, support teams, all employees, and community emergency response organizations. While such exercises are disruptive and may be costly in terms of paid hours diverted from income producing activities, they are useful in spreading awareness of appropriate responses beyond emergency responders and in reinforcing correct responses among emergency responders. All members of the organization should be involved in some training sessions. It is not enough to provide everyone with written guidelines of what to do during various types of emergencies that, if read at all, are quickly filed away and forgotten or lost. With the threats facing organizations in America today, it is necessary to train people to respond to instructions to take cover inside secure buildings, to don appropriate personal protective equipment, and to undergo decontamination procedures if deemed necessary by emergency incident commanders.

Training for the organization's internal emergency response team members must be frequent, flexible, and involve realistic exercises and drills. In actual disasters, classroom-only trained personnel have been known to freeze, panic, and forget everything they were taught. Reactions to disaster situations need to become automatic, and they need to be correct the first time. There is no substitute for regular training several times a year.

IV. A CASE STUDY: MESA STATE COLLEGE

Thus far this paper has covered the threats of terrorism and given prescriptions for dealing with the threats. However, complacency can be a major impediment to implementing any of these prescriptions in an organization, especially when people feel so safe in their local environment that terrorist threats are thought to only involve people in other parts of the world, and during economically difficult times when talent, time, and money to address security issues are all in short supply. The experience of Mesa State College, which has faced both of these impediments, may provide insights to other organizations that are contemplating or dealing with security issues.

Mesa State College is located in a thinly populated pastoral area of farms, orchards, ranches, and federal lands in Western Colorado, about 250 miles away from the major cities of Denver to the east and Salt Lake City to the west. Although attempts of unknown computer hackers to hijack the campus computer network to launch attacks elsewhere, corrupt files, or simply to deny service to campus users had been an ongoing problem, which the Computing & Network Systems Department had kept at bay, no college emergency response plan existed prior to 2001 concerning other types of vulnerabilities to terrorism, and none was thought to be necessary.

In 2001, a telephone call to campus stated that a bomb had been placed in an unspecified campus building. The call prompted a total campus evacuation order and a room-by-room search of all buildings by the police bomb squad. Fortunately, no bomb was found, and later it was discovered that a disgruntled former employee of the college had made the threat. In effect, the entire campus community and local emergency services had been forced to undergo a full-scale exercise simulating an emergency, and the responses of untrained staff and students were troubling. While dormitory staff trained in fire evacuation procedures could be seen with bull horns keeping groups of students together and leading them in an orderly manner to marshalling points off campus, elsewhere the evacuation order was implemented by department secretaries simply walking from classroom to classroom and office to office to notify people to leave buildings. Restrooms were sometimes overlooked, some staff ignored the evacuation order, and some students took their time in exiting, with many either casually milling around outside the buildings awaiting classes to resume, or leaving campus and creating congestion on streets around campus that could have been needed for emergency vehicle access.

Shortly after the bomb threat incident, an ***Emergency Operations Response Plan*** for the college was developed based on the Federal Emergency Management Agency ***Emergency Management Guide for Business & Industry***, and responsibility for implementing the plan was given to the Environment, Health & Safety Committee co-chaired by the Director of Facilities Services and a Grand Junction Police Officer assigned to the college. After the plan was discussed by committee members it became apparent that few college staff had the skills or training to be helpful in dealing with a terrorist-caused emergency, with the exception of School of Nursing faculty who could assist in medical matters, food and housing staff who could assist in shelter matters, and Facilities Services staff who could assist in emergency utility shutoffs, damage assessments, and repairs. Thus, the committee decided to focus on those elements of the plan that could be implemented quickly and to defer elements of the plan requiring far more time, training, and resources to implement. Those elements of the plan that could be implemented quickly included preparing to evacuate all staff and students to assembly points or shelter in an orderly way, and on verifying and compiling up-to-date building blueprints, inventories of hazardous materials in laboratories and shops, and locations of utility shut offs to make available to emergency response services.

Emergency wardens were assigned for every floor and wing of every building on campus, and reverse 911 lines were installed on their telephones to allow the campus command team to issue instructions simultaneously and directly through every warden's telephone, which would act as a loud speaker without requiring the receiver to be lifted. All wardens participated in a training exercise and were equipped with fluorescent vests so that they could be easily recognized and hopefully obeyed. Up-to-date building blueprints were compiled quickly, but much effort was required in the hazardous materials area partly because of staff turnover. Successive drastic cuts to college funding, a hiring freeze, and layoffs in facilities services slowed momentum.

A heightened state of national terrorism alert during the 2003 war in Iraq brought a visit from the County Emergency Manager, who explained how the federal, state, county, and city officials and emergency response professionals would interface with officials of the college. Committee members updated lists of emergency team members and phone numbers following recent layoffs and reorganizations, found money to buy an emergency two-way radio and a bullhorn for the college president, began to check the adequacy of the contents of all first aid kits on campus, began to prepare evacuation kits for building evacuation wardens, developed an evacuation and transport plan for small children in the campus day care center, and trained or re-certified custodians and other interested staff in CPR and first aid.

Two years have passed since the bomb threat triggered serious preparation for a terrorist threat or any other disaster related emergency. Significant progress has been made, but much remains to be done. More personnel need to become involved and to be adequately trained and equipped to take care of themselves and others in the event of a terrorist attack or any other disaster emergency before emergency responders arrive, and then support emergency responders after they arrive. One may still ask whether the college, because of its remote location, really should concern itself with chemical, biological, or nuclear threats. If one considers that the college is located a few miles from an east-west main line of the Union Pacific Railroad which transports hazardous chemicals, a few miles from Interstate 70 that was recently designated a route for transporting nuclear waste to a Nevada repository, and that epidemics such as SARS can turn up anywhere, anytime, a prudent person would say yes.

V. CONCLUSION

Terrorism is a threat that we will likely have to live with for a long time. Rather than let it take control of our lives and activities, we can take preventative and emergency response precautions to minimize the impact it has on our lives. Moreover, natural disasters and accidents without motive occur at random all the time. Even though the odds of being directly affected may be low, consequences can be so severe to such a large number of victims that not to prepare is irresponsible. Preparation is not something that happens overnight by executive decree, even with the full support of organizational members and unlimited resources. Even under orders from the President of the United States and with the full resources of the federal government, it took over a year to complete the initial stages of establishing reliable security at the nation's major airports after the terrorist attack on September 11, 2001. Preparation takes a sustained effort and a commitment of resources over time, which may be counted in years. If your organization has not started to prepare, the time to start is now. Just meeting with representatives of your local emergency response services to find ways to mutually assist one another is a good way to begin.

APPENDIX 1

Steps to Prepare for Disasters (Federal Emergency Management Agency, 2000)

- Establish a planning team
  - Line management and human resources manager
  - Safety, security, and medical personnel
  - Public information officer
  - Support services managers
  - Community emergency response organization managers
- Analyze capabilities and hazards
  - Potential emergencies and probabilities
  - Human impact, property impact, and business impact
  - Internal resources available and adequacy to deal with an emergency
  - External resources available and other priority areas they must serve
  - Resource gap closing additional emergency procedures, training, equipment, and mutual aid agreements
- Develop an emergency operations response plan.
  - Direction and control
    - Incident Commander (IC) to oversee all technical aspects of incident response activities and IC succession plan
    - Protocols with outside emergency response organizations to turn over incident command and coordinate organizational support
    - Emergency Management Group (EMG) of senior managers who can allocate internal resources relevant to the emergency to the IC and are authorized to interface with outside agencies and the media
    - Emergency Operations Command Center (EOC) in a secure area where IC and EMG gather with necessary communications equipment and materials available, including an alternate location
  - Communications
    - Alarms understood by employees to notify of a type of emergency
    - Warning procedures to notify customers and visitors on premises
    - EOC communications to mobilize internal teams of emergency responders,

coordinate with external emergency response organizations, and respond to inquiries from employees' families, neighbors, and the media

- Life safety
  - Authority to order evacuation or to proceed to shelter
  - Evacuation routes and exits clearly marked and well lit
  - Wardens to assist others
  - Assembly areas to account for those present and missing persons to be reported to the EOC with last known locations
  - Search and rescue operations
- Property protection
  - Fire protection systems
  - Automatic shutoffs and emergency power
  - Fire resistant furnishings
  - Securely attached lights, cabinets, and heavy objects
  - Window coverings to protect from flying glass
  - Authority to order facility shutdown and shutdown procedures
  - Vital files and equipment secured or moved to a safe location
  - Restriction of reentry
- Community outreach
  - Review of emergency plans with emergency response groups
  - Facility walk-through and drills with emergency response groups
  - Mutual aid agreements with local response agencies and businesses to receive or provide resources
  - Media briefing area and authorized spokesperson
- Recovery and restoration
  - Maintaining security at the incident scene
  - Initial assessment of damage and remaining hazards
  - Coverings for openings in building to protect undamaged property
  - Insurance coverage and insurance adjuster visits to the incident scene
  - Priorities for bringing utility systems back on-line
  - Salvage operations to segregate damaged and undamaged property
  - Priorities for repairing or replacing equipment
  - Plan for temporarily relocating operations to an alternate site
  - Established lines of succession for key personnel
  - Continuation of employee pay and benefits and crisis counseling
- Administration and logistics
  - Maintaining detailed records of plans, training, and drills
  - Maintaining detailed records of incident events, accounting for personnel, and notification of family members
  - Documenting recovery investigations and operations and managing finances
  - Stockpiling emergency supplies, acquiring emergency equipment, designating command center and alternate site, designating and stocking shelters
  - Providing utility and floor plan maps to emergency responders
  - Providing material safety data sheets
  - Arranging for backup equipment, medical support, food and transportation, and backup communications

REFERENCES

Associated Press. 1998. The Unabomber Case. January 22.

BBC News. 2003a. Seventh Arrest in Ricin Case. January 8.

BBC News. 2003b. Ricin Found in Paris. March 21.

Begley, S. 2001a. Go Well Beyond "Well Prepared". ***Newsweek,*** 138(19): 33.

Begley, S. 2001b. Make Safeguards Go with the Flow. ***Newsweek,*** 138(19): 40.

Boettcher, M., & Arnesen, I. 2002. Al Qaeda Documents Outline Serious Weapons Program: Terrorist Group Placed Heavy Emphasis on Developing Nuclear Device. ***CNN,*** January 25.

Crime Library. 2002. The Aum Cult of Terror: Weird Science. ***Crimelibrary.com.***

Farah, D. 2002. Arrest Aids Inquiry into Arms Network. ***The Washington Post,*** February 26.

Federal Emergency Management Agency. 2001. ***Emergency Management Guide for Business & Industry.***

Hughes, P. M. 1998. ***Global Threats and Challenges: The Decade Ahead.*** Hearing of the Senate Select Committee on Intelligence. January 28.

Johnston, D., Van Natta Jr., D., & Miller, J. 2002. Qaeda's New Links Increase Threats From Global Sites. ***The New York Times,*** June 16.

Magnusson, P., Borus, A., Cohn, L., Barrett, A., Smith, G., Arndt, M., & Zellner, W. 2001. Guarding America. ***Business Week,*** November 19: 34-37.

Maniscalco, P. M., & Christen, H. T. 2002. ***Understanding Terrorism and Managing the Consequences.*** Upper Saddle River, NJ: Prentice Hall.

Mesa State College. 2001. ***Emergency Operations Response Plan.***

Miller, M., & File, J. 2001. ***Terrorism Factbook: Our Nation At War!*** Peoria, IL: Bollix Books.

Minihan, K. 1998. ***Information System Security.*** National Security Agency.

Molander, R. C., Riddle, A. S., & Wilson, P. 1996. ***Strategic Information Warfare: A New Face of War.*** Rand Corporation. Document MR-661-OSD.

Murakami, M. 1998. The Cult that Won't Die. ***Asia Week,*** December 18.

National Commission on Terrorism. 2001. ***Countering the Changing Threat of International Terrorism.*** Report pursuant to Public Law 277, 105th Congress.

Schuster, H. 2003. FBI: Olympic bombing suspect arrested (Eric Robert Rudolph). ***CNN.*** May 31.

Stephenson, J. 1996. Confronting a biological Armageddon: Experts tackle prospect of bioterrorism. ***Journal of the American Medical Association,*** 276: 349-351.

Terrorism Files. 2002. Terrorist Organizations—Aum Supreme Truth. ***Terrorismfiles.org***.

United States District Court for the Central District of California. 1996. ***United States of America versus Kevin David Mitnick and Lewis DePayne.*** CR 96-881.

Verton, D. 2001. Record Year for Security Breaks Expected. ***CNN.*** November 26.