

SECURITY PLAN FOR INDOOR ARENA, USA

Title: Security Plan for an Indoor Arena, Anywhere USA

Author: Jonathan H. Doyle and Phillip C. Durbin

Webster University

Acknowledgement

We would like to thank Tom Hansen, Founder and Chief Executive Officer and Fred Lardaro, Executive Director, Business Development, of AirVisual Inc. for their help and allowing us to use their company's product information in the design of our security plan. Their assistance was invaluable and helpful in designing a structural and technologically integrated security and response plan.

We would also like to thank Major Tom Dailey, Kansas City, Missouri Police Department for his assistance, direction and expertise in the development of critical incident response management.

Abstract

This is a proposed generic security plan for an indoor arena in a moderate to large size city, located within the United States. The goal of this project is to develop a security plan that can be tailored to meet the needs of a security staff for an indoor facility anywhere in the United States. This project addresses: the risks and threats that may affect an indoor facility and its personnel, mitigation applications to reduce the risks and impact of threats to the indoor facility and its personnel, and the development of response and management procedures for critical incidents that could have a major impact on personnel and the surrounding community.

CONTENTS

Table of Figures	v
Situational Analysis	1
Problem Statement	2
Key Definitions	3
Disclaimers, Constraints or Study Limitations	4
Risk/ Vulnerability Assessment	5
Mitigation and Physical Security	26
Critical Incident Response Procedures	38
Conclusion	50
References	50
Appendix A: Department of State List of Foreign Terrorist Organizations	54
Appendix B: Example CARVER Assessment Worksheet	56
Appendix C: Sample Bomb Threat Report	62
Appendix D: Types and Classifications of Fire Extinguishers	64

Table of Figures

Figure 1: Example of Intelliviewer™ Mobile Command System	33
Figure 2: Example of layered defensive measures	37

Situational Analysis

September 11, 2001 had devastating effects on the United States, bringing security to the forefront of peoples' minds both in Law Enforcement and Private Security. Large public events could become the preferred targets or opportunities for terrorist or criminal elements to attack, creating fear, panic, and destruction aimed at crippling the American people's way of life. In this paper we will develop a security plan for a generic indoor arena designed to protect the populous and the facility against man-made incidents and natural disasters and the response procedures dealing with these incidents.

Problem Statement / Premise

To develop a security plan for a generic indoor arena, located in the United States, which addresses the security concerns of the city and surrounding community. This plan will cover: risk and vulnerability assessments, risk mitigation and physical security, and incident response procedures and management. The plan describes the operational structure, resources and procedures that may be activated in response to an actual or threaten critical incident.

Key Definitions

Agro-terrorism- a subset of bioterrorism, and is defined as the deliberate introduction of an animal or plant disease with the goal of generating fear, causing economic losses, and/or undermining stability.

CONUS- Continental United States

CPTED- Crime prevention through environmental design

Hactivism- A form of cyberterrorism

IA- Information Assurance

IED- Improvised Explosive Device

IT- Information Technology

PKI- Public Key Infrastructure

OCONUS- Outside Continental United States

VBIED- Vehicle Borne Improvised Explosive Device

Work Place Violence -Any violent acts, including physical assaults and threats of assault, directed toward persons at work or on duty.

Disclaimers, Constraints or Study Limitations

This plan is designed towards a generic facility and is not a security plan of an existing facility.

Any likeness to any site or city are purely coincidental and may contain redacted information in order to maintain a classification of unclassified and not Law Enforcement Sensitive.

Risk/ Vulnerability Assessment

A hazard is defined as a “source of danger that may or may not lead to an emergency or disaster and is named after the emergency/disaster that could be so precipitated.” Risk is defined as “susceptibility to death, injury, damage, destruction, disruption, stoppage and so forth.” Disaster is defined as an “event that demands substantial crisis response requiring the use of governmental powers and resources beyond the scope of one line agency or service” (Haddow & Bullock, 2006, p. 19).

The nature and types of threats to the American people vary widely with geographic location, criticality of the assets, vulnerability of the target, and level of hostile intent. Nationwide, the serious incident reports consisted of vandalism and violence, disgruntled employee threats, militant jihadist threats to facilities and personnel, U.S. border infiltrations, domestic and international elicitation attempts, international identity theft, organized protests, surveillance, bomb threats, theft, and shootings. All citizens of the United States or those visiting the United States are susceptible to terrorist or criminal attacks. A methodology to determine threats and vulnerability of specific location is the CARVER Methodology and the MSHARPP. (Examples of a CARVER Assessment worksheet see Appendix B).

(A) Criminal.

(1) Threat. Criminals use primarily unsophisticated means of attack and focus on crimes of opportunity. Their goals are to profit from the theft of, or to damage, destroy or disrupt personnel, property, and information. Criminal threats consist of: unsophisticated criminals, saboteurs, gangs, and organized groups. Nationally, criminal activities directed against citizens include vandalizing and shootings, vandalizing facilities, and vandalizing or stealing equipment. **Most criminal threats directed at U.S citizens and guests are unsophisticated and are crimes of opportunity. Many are**

committed by employees and contractors who have the ability to circumvent security systems. These insiders act alone and their acts do not require detailed planning.

(2) Assessment. Indoor Arena, USA has a general, non-specific threat from unsophisticated criminals, saboteurs, gangs, and organized criminals. The threat from saboteurs, gangs, and organized criminals is considered LOW. Due to the ease of action, probability of success, and past history on other like facilities within the U.S, the likelihood of an incident by unsophisticated criminals on personnel, property, or facilities is rated a MEDIUM.

(B) Protestors.

(1) Threat. Protestors conducting protests at facilities and events attempt to garner emotional responses from employees, performers, and family members, or media coverage, often by using offensive language and images to incite a response. The majority of protest groups are non-violent and non-threatening. However, some groups often intentionally break the law in order to be arrested or to disrupt activities.

A religious group that has been protesting events in the United States is the Westboro Baptist Church (WBC). The WBC does not use violence to spread their message. However, their goal at events is to disrupt by provoking others into violence against them via graphic and inflammatory slogans, signs, and verbal harassment. The WBC is very aware of the legal system and uses lawsuits (against those who attack them or otherwise violate their rights) to fund ongoing activities. Additionally, the WBC has a history of filing frivolous lawsuits as a method of harassment (www.adl.org/special_reports/wbc/default.asp). The attendance of WBC at an event will require additional security education and rehearsals, as well as coordination with local Law Enforcement Agencies (LEAs) in order to preclude violence.

(2) Assessment. Continued protest activity will occur against guests, employees, performers/ athletes, facilities, and events. The risk to personnel and property from protests is LOW.

(C) OCONUS Terrorism.

(1) Threat. During the last year there have been a number of threat warnings. Many of these threat warnings are issued with the admonition of there being no "specific, credible threat". From a threat assessment viewpoint, one thing to keep in mind is that the absence of a "specific, credible threat" does not equate to the absence of a threat. For the most part, the threat warnings issued over the past few months concern legitimate tactics and targeting that may be employed by al-Qaeda and other foreign terrorist groups. Tactics and targeting will evolve as U.S. vulnerabilities are exposed and mitigated.

(a) Militant Jihadists: Militant Jihadists pose a significant threat to citizens in selected regions of the country, specifically the east and west coast metropolitan areas. Militant Jihadists attack vulnerable, soft, and unprotected targets which focus on U.S. political, economic, and security interests. These attacks are usually lethal and intended to inflict mass-casualties. Common Militant Jihadist attack methods include: kidnapping, bombing, shooting, arson, hijacking, seizure, raids/attacks on facilities and information warfare.

(b) There are several domestic and foreign organizations which appear to be operating within the U.S. to support an international Islamist revolutionary movement. In 2007, federal agents uncovered a terrorists plot to attack a federal installation on the East coast. International terrorists may utilize the same techniques to attack a high profile sporting event or other large event.

(c) Heightened awareness, increased vigilance and reporting of suspicious activities are strongly encouraged to prevent attacks on personnel or facilities.

(d) Other: Several terrorist groups such as Hamas, which have yet to target U.S. interests, currently operate in the U.S. in a fund raising and recruiting capacity. Additionally, there are many legitimate Muslim organizations (such as Jamaat al' Tabligh) in the U.S. that have been infiltrated by radical Islamic elements. (www.mail-archive.com/islamcity@yahoo.com/msg07118.html). Members of these groups acting alone, or under instruction from superiors, may see an opportunity to damage U.S. foreign policy, by alarming the public.

(2) Other OCONUS Groups may also have a presence in the U.S., but do not currently present a danger. (For a list of OCONUS Groups listed by the State Department See Appendix A).

(3) Assessment. Due to the increased security in larger metropolitan areas terrorists may shift to smaller cities and states where they feel security is easier to penetrate. A terrorist act against any facility or arena would have an impact on Indoor Arena, USA. For this reason the facility is considered to have a general, non-specific threat with the likelihood of foreign terrorist attack being LOW.

b. Domestic Terrorism

(1) Threat. There has been a dramatic decline in activity among the associated anti-government/anti-tax/racist groups in the United States. Most groups, domestic terrorist organizations and "lone wolf" extremists continue to represent a significant threat against the United States. Viewed by some of these groups as symbols of the government, large public

facilities paid for with public tax dollars, their personnel, and equipment may be targeted. The majority of adherents anti-government groups belong to one or more of the following:

(a) Christian Identity. Christian Identity is a religious ideology popular in extreme right-wing circles. Adherents believe that whites of European descent can be traced back to the "Lost Tribes of Israel." Many consider Jews to be the satanic offspring of Eve and the Serpent, while non-whites are "mud peoples" created before Adam and Eve. Its virulent racist and anti-Semitic beliefs are usually accompanied by extreme anti-government sentiments. Despite its small size, Christian Identity influences virtually all white supremacist and extreme anti-government movements.

(b) Ku Klux Klan. Once America's preeminent terrorist organization, the Ku Klux Klan today is a fragmented and amorphous collection of independent groups and individuals, squabbling over diminishing memberships and limited resources. Passed over by most young white supremacists, who consider Klansmen to be ineffectual and faintly ridiculous old-timers, the group presents far, less of a threat to public order than at any time in the past century. Given that some members of the KKK espouse antigovernment views, the gathering of weapons, although legal, may represent a possible threat to U.S. citizens and facilities.

(c) Militias. The militia movement is a right-wing extremist movement consisting of armed paramilitary groups, both formal and informal, with an anti-government, conspiracy-oriented ideology. Militia groups began to form not long after the deadly standoff at Waco, Texas, in 1993; by the spring of 1995, they had spread to almost every state. Many members of militia groups have been arrested since then, usually on weapons, explosives and conspiracy

charges. Although the militia movement has declined in strength from its peak in early 1996, it remains an active movement, especially in the Midwestern and Northwestern US.

(d) Posse Comitatus. The "sovereign citizen" movement is a loosely organized collection of groups and individuals who have adopted a right-wing anarchist ideology originating in the theories of a group called the Posse Comitatus in the 1970s. Its adherents believe that virtually all existing government in the United States is illegitimate and they seek to "restore" an idealized, minimalist government that never actually existed. To this end, sovereign citizens wage war against the government and other forms of authority using lawsuits and court filings in order to harass and intimidate, and occasionally resort to violence (www.nizkor.org/hweb/orgs/american/adl/paranoia-as-patriotism/posse-comitatus.html).

(e) Tax Protest Groups. The tax protest movement is a relatively long-lived anti-government movement rising out of opposition to federal income taxes. Tax protesters generally believe that either the income tax laws are in some way invalid or that they do not apply to most citizens; therefore, they believe they have a legal and moral right not to pay taxes. Many tax protesters suspect that the government covers up the "truth" about the income tax in order to continue oppressing the people and taking their money. Tax protesters engage in a wide variety of tax evasion strategies that range from simple refusal to pay taxes to complicated schemes using onshore and offshore trusts in order to hide income from the government. Tax protesters are also violent on occasion, attacking IRS agents or property or others charged with enforcing the law. With the trend of cities to build new facilities with public money this could draw attention of these groups.

(f) Neo-Nazi groups. Neo-Nazi groups share a hatred for Jews and a love for Adolf Hitler and Nazi Germany. While they also hate other minorities, homosexuals and even sometimes Christians, they perceive "the Jew" as their cardinal enemy, and trace social problems to a Jewish conspiracy that supposedly controls governments, financial institutions and the media. In the past the most important neo-Nazi group in the U.S. is the National Alliance. Until his death, it was led by William Pierce, the infamous author of the futuristic race-war novel *The Turner Diaries*, a book believed by some to have served as the blueprint for the 1995 Oklahoma City bombing (www.aijac.org.au/review/2000/258/sounds.html). With the death of Pierce, the National Alliance began to fall apart. However, under new leadership, the National Alliance has begun to become more active, utilizing "Trojan Horse" recruiting, by organizing Irish cultural events from New Jersey to California as a way of exposing "European culture and young whites to a "white culture" they might not have seen before." The events are held by the "European Cultural Association," a front for the National Alliance. It is possible that extremist within the Neo-Nazi movement or "lone wolves," inspired by the movements propaganda could resort to violence. Other active offshoots of the Neo-Nazi ideology include:

1. Racist Skinheads. Racist Skinheads form a particularly violent element of the white supremacist movement, and have often been referred to as the "shock troops" of the hoped-for revolution. The classic Skinhead look is a shaved head, black military style boots, jeans with suspenders and an array of typically racist tattoos. The leading racist skinhead group is currently the Hammerskin Nation. Racist Skinheads activity is often centered on the white power music industry, such as "Panzerfaust" Records and "Resistance" Records.

2. Nazi Low Riders (NLR). The NLR is a violent gang which emerged from former inmates of the California Youth Authority. The group makes an exception that appears to

run counter to their staunch white power beliefs — they allowed a relatively small number of Latinos to join. Latinos not only boosted the size of the group, they also did much of the dirty work, trafficking drugs like methamphetamines inside and outside of prison. Currently experts estimate that it has 1,000 active members, most of them behind bars in California, Arizona, Nevada, Utah, Oklahoma, Illinois and Florida. Members are primarily recruited in juvenile and adult prison facilities while in their teens and early twenties (www.en.wikipedia.org/wiki/Nazi_Lowriders).

3. Public Enemy Number One (PEN1). PEN1 is the fastest-growing Caucasian prison gang, with an estimated 400 to 500 members operating in prisons and communities in California and, to a much lesser extent, in locations throughout the northeastern, Pacific, southwestern, southeastern, and west central regions of the country. PEN1 members espouse a white supremacist philosophy and pose a criminal threat in and outside prison because of their alliance with Aryan Brotherhood (prison gang) and NLR. Gang members derive their income from distributing midlevel and retail-level quantities of methamphetamine. In addition, members engage in violent criminal activity such as assault, attempted murder, and homicide as well as auto theft, burglary, identity theft, and property crimes (www.adl.org/main_Extremism/peni_california_racist_gang.htm).

(2) Assessment.

(a) While there seems to be a significant decrease in the activities of anti-government/anti-tax/racist groups within the last three years, it is more likely that the manner in which they recruit and share information has changed. The rise of the internet has given a somewhat anonymous and low cost / low risk way of distributing ideas, raising money, and

recruiting members. There is no longer a need to hold meetings and rallies to express their views. However, many white power groups are now using the issue of state sanctioned gay marriage to recruit member and form protests.

(b) While anti-government beliefs are a fundamental tenet of all these groups, these groups show no indications to move beyond the rhetoric and resort to violence. Any violent act perpetrated by these organizations is likely to be directed against individuals or as random acts of vandalism against property. The threat of a domestic terrorist attack by these organizations is low, but there is still the threat of a domestic terrorism throughout the United States against facilities such as the Indoor Arena.

(c) It is believed that the number of active members in each of these organizations is extremely small. Issues that would be a catalyst for growth/activity of these organizations would be the illegal immigration issue or a farm crisis (similar to the 1980's) that resulted in multiple farm foreclosures, and/or a general economic downturn in the U.S., and/or to a lesser extent, the gay marriage issue.

(d) The facility is considered to have a general, non-specific threat with the likelihood of domestic terrorist attack being LOW.

c. Eco-Terrorism

(1) Threat. During the past two decades in the U.S., radical environmental and animal rights groups have claimed responsibility for hundreds of crimes and acts of terrorism, including arson, bombings, vandalism and harassment, causing more than \$100 million in damage. While some activists have been captured, eco-terror cells - small and loosely affiliated - are extremely

difficult to identify and most attacks remain unsolved. Although it has been overshadowed by Islamic terrorist threats since September 11, eco-terrorism remains one of the country's most active terrorist movements. The most active groups are Animal Liberation Front (ALF), Earth Liberation Front (ELF), Stop Huntingdon Animal Cruelty (SHAC)

(a) The Animal Liberation Front (ALF), and Earth Liberation Front (ELF) share a common belief system and have connections to each other. More importantly is the fact that ELF has been reported to have had connections to al-Qaeda. Both groups are generally non-violent but have conducted acts of vandalism in the past. This includes a 2004 attack on the University of Iowa, Psychology Department's research of facilities that resulted in the removal of research animals and over \$100,000 in damage (www.animalliberationfront.com/ALFront/Actions-USA/iowabreakin.htm).

(b) Groups such as ALF publish manuals on their website on gluing locks; damaging vehicles, telephone lines and security cameras, conducting surveillance, arson, and creating timers for incendiary devices. Another manual provides step-by-step instructions and diagrams for preparing various igniters and incendiary devices, as well as home-made napalm. Such devices have been used in numerous attacks.

(2) Assessment

(a) Terrorism in the name of animal and environmental protection has steadily increased during the past decade in the United States. Automobile dealerships, forestry companies, corporate and university-based medical research laboratories, restaurants, medical-supply firms, fur farms, plant genetic research facilities, and other industries continue to be targeted. Of concern is the possibility of anti-capitalist/anti-government elements within the

radical environmentalist movement could target symbolic government/public facilities, to include the Indoor Arena.

(b) Animal rights groups' publications and web sites have shown an increase in violent rhetoric as well as anti-capitalist and anti-modernization statements. Although no one has yet been injured in a domestic eco-terror attack, the increasingly violent nature of these of attacks suggests that someone will be hurt before long.

(c) Due to recent attacks and the nation's dependence on domestic agriculture, the Indoor Arena is considered to have a general, non-specific threat with the likelihood of eco-terrorist attack being LOW.

d. Cyber Security Threats.

(1) Threat. The very linkages that enable information technology (IT) systems to function also provide vulnerable points that can be exploited. The dependence on the systems' functioning as planned is a source of great vulnerability.

(a) A physical threat to tangible property, such as the theft or destruction of computer hardware exists.

(b) In most cases, the target of the threat is the information itself rather than the system that transports it. Threats include computer crime, computer espionage, "hacktivism", and cyber terrorism. Types of cyber security attacks may include: probes, scans, account compromises, root compromises, packet sniffing, denial of service attacks, exploitation of code, and internet infrastructure attacks (Krutz & Vines, 2007, pp. 61-68). The goal of these attacks are data destruction or corruption, penetration of a system to modify its output, theft, disabling a

system, taking control of a system, and website defacement. The greatest threats to cyber security are (in order): insiders, hackers, and terrorist/criminals.

(2) Assessment. The U.S. is considered to have a general, non-specific threat, with the likelihood of cyber security attack being MEDIUM. Due to information security measures in place, the Indoor Arena has general non-specific threat with the likelihood of a successful cyber security attack being LOW.

e. Weapons Of Mass Destruction (WMD).

(1) Threat. WMD are classified as chemical, biological, radiological, nuclear, or high yield explosive (CBRNE). A WMD attack in any of these states would have an impact on the nation as a whole and an attack on a state neighboring the state the Indoor Arena is located in would have an effect on the arena as well. Anthrax attacks represent a risk. Most facilities do not have a mail room separated from heating, ventilation, and cooling (HVAC) systems. The contents of any opened letter or package would quickly spread and contaminate the entire facility. Due to the difficulty in weaponizing Anthrax, it is more likely that false Anthrax attacks or so called “White Powder incidents” will occur (www.schneier.com/blog/archives/2005/06/white_powder_an.html).

(2) Assessment. For the above reasons, the U.S. is considered to have a general non-specific threat with the likelihood of WMD attack being MEDIUM. It is possible that facilities may have “White Powder” incidents, especially copy cat attacks after publicized national “White Powder” incidents. The Indoor Arena is considered to have a general non-specific threat of WMD attack with the likelihood of being LOW.

f. Bomb Threat.

(1) Threat. Bombing, by Improvised Explosive Device (IED), Vehicle Borne Improvised Explosive Device (VBIED), or Mail bomb is a method of terrorism shared by domestic and international terrorists, and in some cases eco-terrorists. Typically, the size and ability of the organization determines the size of the bomb. A larger, more organized group is usually required to successfully construct and deliver a VBIED. (Notable exception being the Oklahoma City bomber) Bombings are a low risk, high pay off method that guarantees media attention. The size of most bomb attacks would be between 25 pounds (suitcase) and 220 pounds (mid-sized car). Unsophisticated criminals and vandals may use pipe bombs of 1-2 pounds. The possibility of a threat by mail or package may be made to the facility or organization. Mail delivery systems may be utilized as a vehicle to create real or perceived danger through several different methods. These threats may be for revenge, extortion, or terrorism. The threats may be contained within the parcels of all shapes and sizes. Mail bombs against public targets were more commonly used during the 70s and 80s, especially by radical leftist groups and notably several Americans were killed or injured by the “Unabomber” who conducted a sporadic mail bomb campaign to “eliminate industrial society” for over 18 years.

(2) Assessment. IED and VBIED are the most dangerous threat to Indoor Arena personnel and facilities. Standard outdoor evacuation distance for a device between 25 lb and 220 lb is 450-560 meters. Standard building evacuation distance for a device between 25 lb and 220 lb is 50-200 meters. Due to lack of past history of actual bombings against arenas in the U.S. and no active threat groups who utilize IED/VBIED/mail bombs, the threat against the Indoor Arena is LOW. The likelihood of a telephonic bomb threat against the Indoor Arena is MEDIUM.

g. Workplace Violence.

Threat. Violence in the workplace is a substantial contributor to occupational injury and death. Nonfatal assaults result in loss of workdays and cost workers in lost wages. The Occupational Safety and Health Act's General Duty Clause requires employers to provide a safe and healthful workplace for all workers covered by the OSH Act (www.cdc.gov/niosh/injury/traumaviol_research.html).

(a) Employers who do not take reasonable steps to prevent violence can be cited.

(b) There are two major categories of workplace violence

1) Physical- which can include: shootings, beatings, suicide attempts

2) Emotional- which can include: threats, intimidating behavior, disruptive behavior, verbal abuse

(c) Risk factors for workplace violence include dealing with the public, the exchange of money, and the delivery of services or goods, working alone or in small numbers, working late at night or during early morning hours, and guarding valuable property or possessions.

(d) Violence in the workplace due to a domestic partner is a threat and the indicators of potential domestic violence include:

1. Employee or co-workers' reports of an employee being injured by a domestic partner.

2. Bruises or physical complaints that show evidence of assault.

3. Emotional outburst while talking with a domestic partner on the telephone or in person at the workplace.

4. Increased absenteeism or reduced productivity.

5. Spouse or partner makes disruptive visits to the workplace

(www.cdc.gov/niosh/injury/traumaviol_research.html).

(e) Other potential types of work place violence at the Indoor Arena include:

1. Fan on Fan violence – due to intoxication or overzealousness in team spirit/rivalry, hate crimes, petty theft, mugging

2. Fan on Employee- due to intoxication or overzealousness in team spirit/rivalry, hate crimes, employees attempting to calm/break up fights between fans, robbery at concession/vendors

3. Fan on Performer- due to intoxication or overzealousness in team spirit/rivalry/taunting, hate crimes, or if the performer enters the seating areas (Ron Artest at The Palace in Detroit, ESPN,2004)

4. Performer on Performer- due to overzealousness in team spirit/rivalry (Albert Haynesworth stomping on a players head during a football game after the opponent's helmet came off) (Sporting News, 2006)

5. Employee on Performer- due to overzealousness in team spirit/rivalry, hate crimes, robbery attempts

6. Past Employees returning to the facility with grudges against the facility or personnel.

(2) Assessment. Within the last five years, there have been several nationally publicized instances or situations that have escalated into work place violence in sports arenas. Based upon historical instances in other similar facilities, the Indoor Arena a MEDIUM risk of violence in the workplace.(ESPN, 2004,)

h. Tornado, Hurricane & Severe Storm Threat.

(1) Threat. The probability of significant weather related activity in the United States varies from state to state, and depends on the location of the Indoor Arena. The effects of a significant weather related activity in a neighboring state may have an impact on the operation of the Indoor Arena.

(a) Tornadoes: Tornado season in the United States is year round. The peak season in the southern states is between March and May and the peak tornado activity in the northern states is during the summer months (www.noaa.gov/tornadoes.html). While tornadoes can appear anywhere, the historical trend is that tornadoes predominantly occur within the Midwest region. There is a less significant risk of straight line winds or microbursts. However microbursts have the potential to cause as much damage as a severe tornado and pose a major risk to personnel and facilities.

(b) The U. S. peak risk of severe thunderstorms and hail generally correspond to the date of peak tornado of activity as described above. However, the likelihood of thunderstorm and hail activity starts in late March and ends in early October.

(c) Hurricanes: Hurricanes season in the United States begins in June and lasts until November with peak hurricane activity in the mid to late August to September timeframe.

(www.aoml.noaa.gov/hrd/tcfaq/G1.html). While hurricanes can appear anywhere along the coastlines of the United States, the historical trend is that hurricanes predominantly occur along the East Coast and the Gulf Coast region. Hurricanes possess a significant potential to cause as extreme damage from high winds and flooding and pose a major risk to personnel and facilities.

(2) Assessment. Based on historical trends and geographic location, the U.S. has a HIGH likelihood of loss of life and/or property due to tornados, hurricanes, severe storms and hurricanes. The threat to the Indoor Arena varies largely on geographic location of the facility within the United States. The facility has an overall LOW threat to life and/or property loss due to tornados, severe storms and hurricanes

i. Winter Weather.

(1) Threat. Winter weather is a large category that may include heavy precipitation (snow, freezing rain, and sleet), extreme cold, and/or strong winter winds.

(a) Winter weather is considered a deceptive threat because most injuries and deaths are indirectly related to the storm. The actual threat depends on the specific situation. Recent observations indicate the following pattern for winter deaths:

1. Related to ice and snow:

a. About 70% occur in automobiles.

b. About 25% are people caught out in the storm.

2. Related to exposure to cold:

a. 50% are people over 60 years old.

b. Over 75% are males.

c. About 20% occur in the home (www.nws.noaa.gov/om/winter/winter1.htm).

(b) Effects of a severe winter storm include.

1. Highways closed or difficult to travel on and increased auto accidents.

2. Difficulty in obtaining medical care (Unable to get to hospital - ambulances blocked by snow-covered roads.)

3. Shipment of food and other goods delayed.

4. Power and communications disrupted because of downed lines.

5. Fire and police delayed in responding to emergencies.

6. Cars hard to start, need assistance.

7. Large costs to state, county, and local highway departments for snow removal.

(c) The U.S., normally, experiences severe winter storms during the November-April period. These storms may be those with only heavy snow, or with snow and ice mixed, or with ice (glaze) only. Historically, the peak risk period for winter storms is in January. Late December and early March also have high incidences of winter storms. However, severe winter storms may occur as early as late October or as late as the first of May.

(2) Assessment. Based on historical trends and geographic location, the nation has a MEDIUM likelihood of severe winter weather that would overwhelm local and/or state resources

or result in a threat to property and/or life. The Indoor Arena has a LOW threat to life and/or property due to severe winter weather.

j. Flooding.

(1) Threat. The United States faces a yearly threat to property, and occasionally life, due to spring and summer flooding. In the Midwest, the Missouri and Mississippi Rivers has had a major flood history in recent years. Other rivers, tributaries and creeks may contribute to flooding in regional areas. The geographic location of the Indoor Arena in relation to these waterways will dictate the threat to personnel and the facility. The effects of a significant flood related activity in a neighboring state may have an impact on the operation of the Indoor Arena as was demonstrated during Hurricane Katrina at the Superdome in Louisiana.

(2) Assessment. Based on historical trends, the United States has a HIGH likelihood of flooding that would result in a threat to property and/or life. Due to the regional nature of the flooding the Indoor Arena has a LOW threat to life and/or property due to flooding.

k. Earthquake.

(1) Threat. The New Madrid Fault Zone, located along the valley of the Mississippi River, and centered near the town of New Madrid, in the boot-heel area of Missouri, produced the strongest historic earthquakes in North America (estimated magnitude of 8.3 to 8.7) between December 16, 1811 and February 7, 1812. (www.quake.ualr.edu/public/nmfz.htm) The San Andreas Fault Zone is a geological fault that runs a length of roughly 800 miles (1300 kilometres) through western and southern California in the United States. The fault, a right-lateral strike-slip fault, marks a transform (or sliding) boundary between the Pacific Plate and the North American Plate.

(www.en.wikipedia.org/wiki/San_Andreas_Fault) Earthquake shock waves travel faster and farther in the Midwest, making quakes here potentially more damaging than similar sized events in other geologic settings. The direct physical effects would likely be minor to moderate, based on the structural design of the facility although they could be more severe if geographically located near the epicenter of the earthquake. Structural damage could include cracked or broken walls and windows, support beams and ceiling rafters; disruption of local gas, water, sewer, and electric utilities; fluctuation of water; local landslides along steep slopes; high water along floodplains; pressure changes in gas-storage facilities; and even sinkhole collapse. The regional effects of a severe earthquake like those of 1811-1812 would constitute a major disaster. The New Madrid and San Andreas Fault Zones are densely populated. Consequences for the Indoor Arena if located within this region would include medical and other evacuations from damaged areas to facilities, and may be required to serve as a shelter for personnel in the stricken areas.

(2) Assessment. Based on recurrence intervals for small earthquakes, scientists estimate a chance of a Richter magnitude 6.0 earthquake at 90 percent by 2040. Estimated recurrence intervals for larger earthquakes, approaching the size of the 1811-1812 events, vary from about 175 years to greater than 700 years. The United States has a MEDIUM likelihood of an earthquake that would result in a threat to property and/or life. If one were to occur, the Indoor Arena may be affected. The Indoor Arena has a LOW threat to property due to earthquake.

1. Food Service

(1) Threat. There have been recent outbreaks of e coli and other bacterial and food borne pathogens throughout the United States at restaurants and grocery stores. (CNN,2006) Many of these contaminants were found in the food at the source or processing plant, but there is a danger

of contamination at the plant prior to packaging and shipping to the vendor. An up and coming threat within the United States is agro-terrorism. Attacks against agriculture are not new, and have been conducted or considered by both nation-states and sub state organizations throughout history. Another threat is the introduction, whether intentional or unintentional, of contaminants in the products at the concessions/ vending areas.

(2) Assessment. Recent events within the United States, there is a MEDIUM likelihood of agro-terrorism/ contamination in the food supply that would result in a threat to life. The risk to the Indoor Arena's food service section due to agro-terrorism or employee contamination is LOW to patrons and employees.

Mitigation and Physical Security

The strategy for risk/threat mitigation and physical security is similar to that of a military defense in depth. The goal is to defeat the threat as early as possible and as far from the facility as possible. This strategy will allow more time for security staff/ local law enforcement to respond to an incident. The defensive plan uses the physical structure and technology which allows for the optimal placement of security personnel at the proper place and time, that creates or tailors the conditions for a favorable response and preventing a critical incident before it occurs. Other reasons for conducting a defense in depth include:

- Retaining decisive terrain or denying a vital area of the facility to unauthorized personnel.
- Fixing or delaying entry into the facility by unauthorized personnel until a suitable response force can arrive at the scene.
- Reducing the risk to the facility of a surprise nature.
- Increasing the intruder/adversary's vulnerability to detection prior to entry into the facility. (www.globalsecurity.org/military/library/policy/army/fm/3-90/ch8.htm).

The indoor arena defense in depth security is accomplished through the following measures; physical structure, crime prevention through environmental design (CPTED), use of security personnel, technology, access control, and information technology defense.

(A) Physical Structure

The first step in mitigating most threats or risks to the facility is through proper design of the physical structure of the building. Many of the risks can be countered just by ensuring that the facility meets or exceeds all Federal, State, and local fire, safety, electrical, health and other applicable codes or ordinances. During the design and construction of the facility, adequate space must be allocated for a Command Center/Emergency Operations Center as a central control hub for all security or emergency operations within the facility and grounds. This begins with the coordination between the facility and the city emergency management, police, fire, and emergency services personnel to establish the needs and requirements of those departments in order to best support the facility and the city's needs.

The facility Command Center needs to be well structured and designed for day to day and emergency operations. It must be capable of being upgraded as new technology evolves, as it is more cost efficient to build from the ground up than to re-design or re-structure after the construction of the facility is completed. The design must include redundant power sources, different forms of communication; fm, cellular, land line, and computer in the event that any of the systems fail. A more cost efficient design would also include having the command center networked into the city's Emergency Operations Center. Additionally based on the exact geographic location of the facility extra precautions may be necessary for added protection specific natural phenomena (ie. flooding, earthquakes, hurricanes, tornados) which are common to the area the Arena is being built. Incorporated into the design of the building should be some measure of crime prevention through environmental design.

(B) Crime Prevention Through Environmental Design (CPTED)

New facilities have been designed by architects that see the need to plan and build with more in mind than just the traditional threats of nature: fire, earthquakes and hurricanes. They must now consider the threat of crime. CPTED is crime prevention through the environmental design of the building and surrounding grounds. As in the design of the Command Center, prior thought and coordination should be included in the design of the exterior of the facility and grounds. Some techniques of CPTED includes; street and security lighting, landscaping, barriers, traffic control measures, and target hardening. CPTED crime prevention principles can be applied easily and inexpensively to the facility during the construction phase. The secret to CPTED crime prevention is a design that eliminates or reduces criminal behavior. These are four major strategies that go into creating an effective CPTED crime prevention environment.

1. Natural Surveillance - A design concept directed primarily at keeping intruders easily observable. Promoted by features that maximize visibility of people, parking areas and building entrances: doors and windows that look out on to streets and parking areas; pedestrian-friendly sidewalks and streets; adequate nighttime lighting.

2. Territorial Reinforcement - Physical design can create or extend a sphere of influence. Users then develop a sense of territorial control while potential offenders, perceiving this control, are discouraged. CPTED measures define property lines and distinguish private spaces from public spaces by using landscape plantings, pavement designs, and natural barrier fences.

3. Natural Access Control - A design concept directed primarily at decreasing crime opportunity by denying access to crime targets and creating in offenders a perception of risk by designing streets, sidewalks, and building entrances to clearly indicate public routes and discouraging access to private areas with structural elements.

4. Target Hardening - Accomplished by features that prohibit entry or access: window locks,

dead bolts for doors, interior door hinges and other access control devices (www.cpted-watch.com/). Additional measures include; adequate standoff distance between vehicular traffic and parking areas and the main arena structure, emplacing barriers (mobile and fixed) to create distance between the building and vehicles greatly increases the survivability of the structure and reduces the risk of vehicle bombs destroying the building and injuring a large number of people and yet remains aesthetically pleasing to the eye.

(C) Prevention through Security Personnel

One of the most important means of protecting the facility and its personnel and guests is professional, competent and fully trained Command Center. The security staff is the front line and the facilities face to the public and its workers. Command Center that are certified and trained to the industry standards are the best way to diffuse situations before they become uncontrollable (Davies, S.J., & Minion, R.R.,1999). The Command Center must be able to interact with the public and have the interpersonal skills needed to work in the security environment and must be able to make calm rational decisions while in stressful situations. The Command Center should be a combination of full time employees and off duty law enforcement officer that have been certified to work in the private security field. The security manager must develop a policy for continual training to maintain the security forces proficiency in both day to day duties and in crisis situations. The security manager must be in close contact and interact with the local police, fire, and emergency services departments and coordinate emergency and response plans for the facility with each agency (Davies, S.J., & Minion, R.R.,1999). The security manager must also coordinate with the local city's emergency operations center and ensure the facility's and the city's emergency plans are coordinated and supported. Part of the

coordination can be done through the facility's Command Center and the software technology being used in the Command Center.

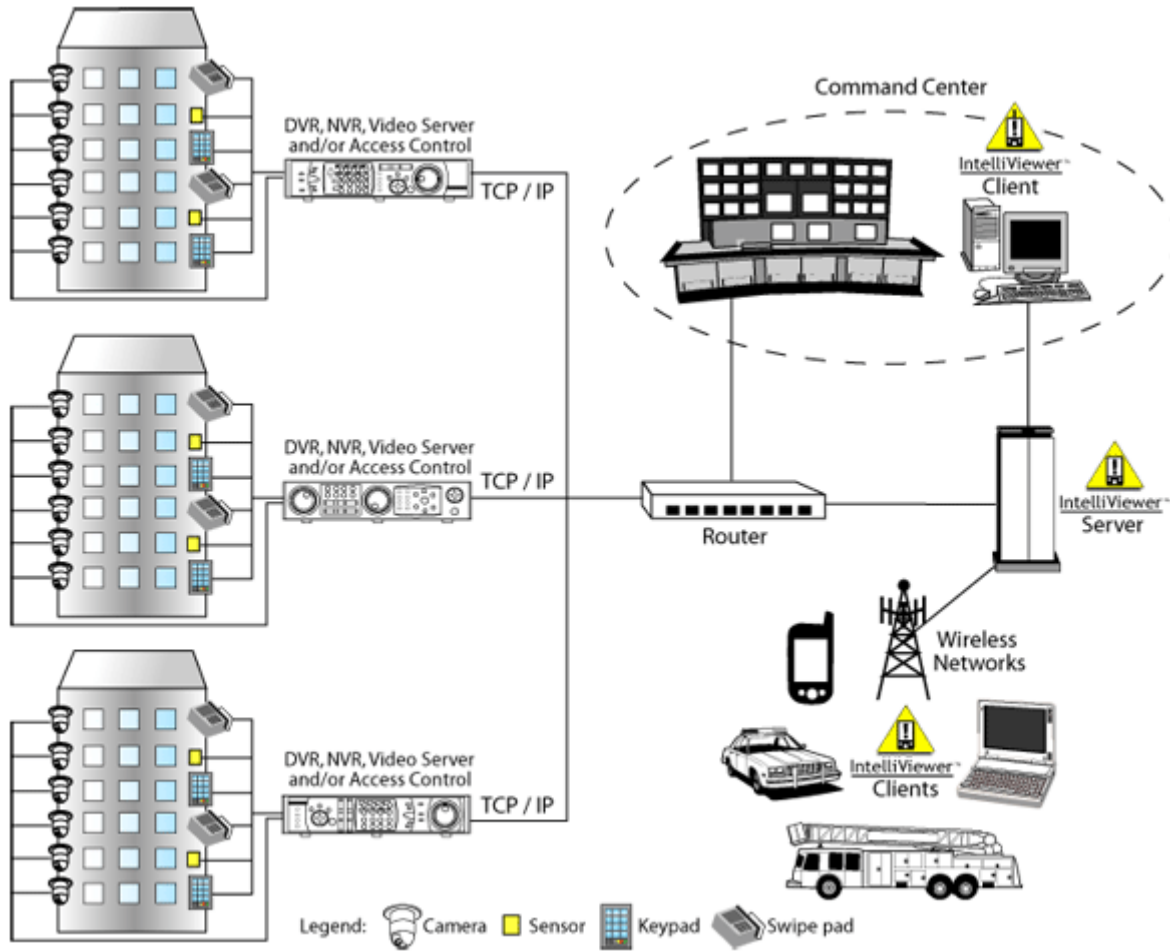
(D) Prevention through Technology

Augmenting the Indoor Arena's trained security personnel will be the application of security technology of the company AirVisual™. AirVisual™ is a wireless application service provider on the leading edge of security software technology. The platform designed by AirVisual™ captures video and location-based data, including real-time or archived video, access control information, audio and text and transmits the information over any cellular, or Wi-Fi or Mesh network, to any off-the-shelf mobile device such as a PDA, cellular phone, notebook PC or desktop (Lardaro,2007). AirVisual™ offers real-time communication and multiple system access and control for those in the field, as well as those in the Command Center. The system gives security personnel the ability to prepare the response by reviewing and sharing crucial video of current and past incidents as well as notifying personnel of vital alerts, safety sensors and security breaches. The AirVisual™ technology provides security operations and mobile command capabilities which will allow for the establishment of alternate Command Center locations to ensure survivability/continuity of operations during a critical incident.

The AirVisual™ system will enhance the CCTV and allow for the customization of the security for each event held at the facility. This customization can be done by adding and/or moving wireless cameras to different locations based on the needs of each event and the desire to add security to more sensitive areas based upon the type of event or dignitary attending a function at the facility. AirVisual™ also ties access control networks to the visual security networks enabling security personnel, first responders and law enforcement personnel to remotely monitor and control video and access control systems from anywhere (Lardaro, 2007).

The AirVisual™ platform combines multiple security components for remote access to real-time visual information and allows personnel in the field to stay mobile and have access to the decisive data without being tied down to a fixed location. Part of the AirVisual™ platform is the IntelliViewer™ wireless video monitoring platform and mobile command system which is a customizable set of software and network services that can accept content from any content feed or security/safety sensors and then deliver the information over the network and display the information on a variety of devices(PDA, cellular phone, notebook etc.) (www.AirVisual.com). Using the AirVisual™ platform software the Command Center has the ability to distribute location-based data (maps and schematics – floor plans, building composition, entrances/exits, etc.) to security personnel and responders to allow for critical decisions to be made faster and to give the responders a better idea regarding the situation they are about to encounter. This saves time and lives by allowing the responders to bring the correct equipment to the incident and to enter the facility at the best possible location to make a positive impact (www.AirVisual.com).

Figure 1. Example of the IntelliViewer™ Mobile Command System



(AirVisual, 2007)

(E) Prevention through Access Control

Access control is a key part of the security program. It is very important to keep unauthorized personnel out of restricted areas and the public out of the facility when there are no events occurring, and will prevent or deter any theft, vandalism, or trespass to the facility. The access control system should include combination of biometrics, keypad/pin, and badges. The biometrics portion of the system will be made up of a thumb scanner with a digital key code on a number pad, also security and staff identification cards will be issued and worn around the neck or prominently displayed while in the facility. The IntelliViewer™ can be utilized to verify employment status and will also allow for a computer log-in database, which can also be used for

accounting purposes, verification of hours worked, and accountability during crisis incidents.

The thumb scanners with number pad will be located at all employee entrances and key locations, restricted to the public. These thumb scanners with number pads can be programmed to grant limited access based on set permissions to individuals based on security clearances and need for access. Additionally the system can be set to control employee access during certain hours or special events based on the security needs. In addition to a computer log, a IntelliViewer™ video log will be created as entry into restricted areas is made, with an electronic date/time stamp.

(F) Information Technology (IT) Defense

Once a basic level of understanding of the defense in depth areas is achieved an organization can begin developing an IA program in accordance with federal standards.

Every level of the network must be protected and the information backbone must be defended to ensure the systems are guarded in order to comply with the strict policies regarding the releasability of information.

Once the environment and the reason why information must be protected is understood, then the organization must characterize their adversaries, the potential motivations of these adversaries and the attack capabilities these adversaries have (Information Assurance Technology Framework, IATF, Release 3.1, September 2002, p. 2-4). The adversaries to the facility network might include; terrorists, hackers, or criminal elements. These attackers may be motivated the need to gather intelligence, theft of intellectual property, embarrassing the organization, or in the case of some hackers just for fun of breaking into the facility network.

There are five types of Information Technology attacks: passive, active, close-in, insider and distribution. Passive attacks include traffic analysis, monitoring unprotected communications,

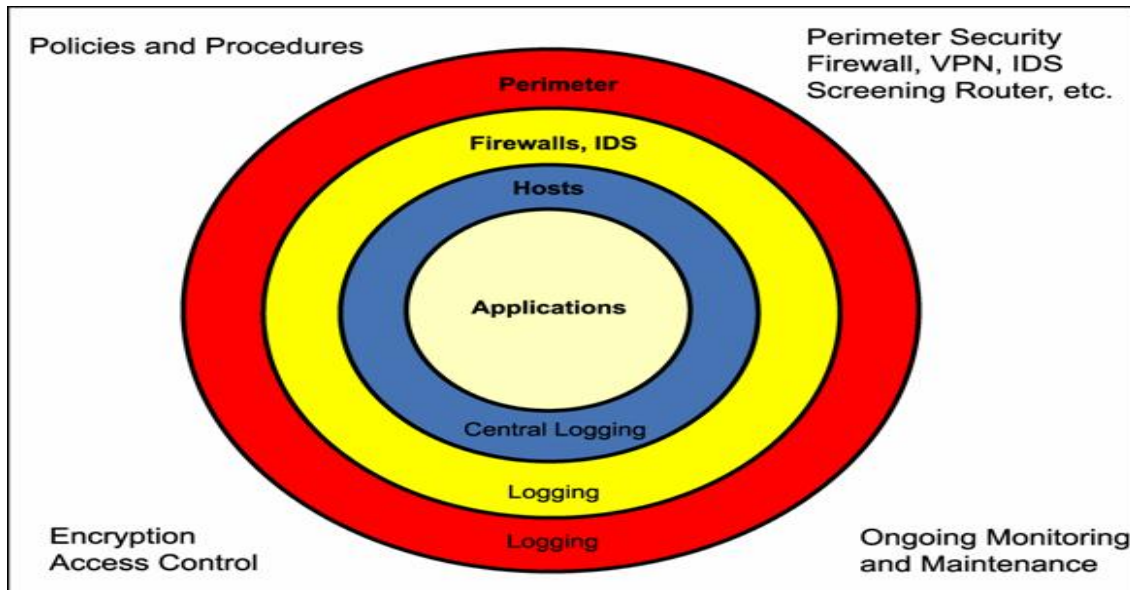
and capturing authentication information (passwords). Passive intercepts can give adversaries warnings of impending actions or can result in disclosure of important files or data without the knowledge of the user (IATF, 2002, p. 2-5). Active attacks include attempts to break the protective features of the system, introducing malicious code, and stealing or modifying information. (IATF, 2002, p. 2-5) These attacks can be mounted against any portion on the system such as the network backbone, an enclave or a authorized remote user trying to connect to an enclave. These attacks can result in disclose of information to unauthorized personnel, denial of service to authorized users or unauthorized modification of data. A third type of attack is the close-in attack. Close-in attacks are made by individuals attaining close physical proximity to networks, systems or facilities for the purpose of modifying, gathering or denying access to information. (IATF, 2002, p. 2-5) The close physical proximity can be achieved by stealth, open access or both. The fourth type of attack is an inside attack. An inside attack can be either malicious or non-malicious. Malicious inside attackers intentionally steal or damage or use information in a fraudulent manner or intentionally deny the access if other authorized users to the information. Non-malicious attacks normally result from lack of attention to policies, ignorance of the policies or intentional workarounds in order to get the job done faster. The last class of attack is the distribution attack. The distribution attack focuses on the malicious modification of hardware or software at the factory or during distribution (IATF, 2002, p. 2-5). These attacks can introduce malicious code allowing unauthorized users access to information on the network at a later date. All five of these types of attacks must be examined and considered during the risk assessment process while designing the network and ways to mitigate or prevents these attack must be implemented to achieve Information Assurance, (IA).

The defense in depth strategy to achieve IA is through the application of security services designed to protect, detect and react to attacks, and one to the key principles to achieving IA is a balanced look at people, technology, and operations. IA cannot be achieved without a commitment by senior level management and their clear understanding of the perceived threats. Once the senior management is on board, policies and procedures can be created, these policies would define the roles and responsibilities of everyone in the organization and define ways violations of the policies would be handled. These policies would also allocate resources for training programs for users at all levels and establish physical and personal security requirements. There are wide range of technological services with can help with IA and detecting intrusions. The key in implementing the technology is have established effective policies and processes for procuring these technologies. These policies should include a security policy, IA principles, system level IA architectures and standards, criteria for needed IA products, acquisition of evaluated products by a reputable third party, configuration guidance and a risk assessment for integrating the new technology (IATF, 2002, p. 2-8). The operations portion of the IT defense in depth strategy focuses on the day to day operations of the organization and their security posture. It focuses on the ability of the organization to enforce its security policy and respond to attacks on its system. The operations focus also looks at the organizations policies and procedures for recovering from an attack and its redundant capabilities to survive the attack and continue operations with the minimum amount of loss in time, information or money.

Everything that is been discussed so far has set the stage which would allow for the execution of defense in depth of facility systems and network. By establishing the policies and getting the senior management buy-in and procuring the right technology can properly execute defense in depth by establishing defense in multiple locations, layered defenses, robust security, deploying

PKI and intrusion detection devices. Establishing a defense in multiple locations realizes that attackers can strike a target from many different directions both internally and externally; this requires an organization to establish protection mechanisms at numerous locations to resist the attacks. At a minimum the defenses should include: defending the networks and infrastructure, defending the enclave boundaries, and defending the computing environment (IATF, 2002, p. 2-12). An organization can not rely on a single mechanism to protect them because every IA product has its limitations and eventually an attacker will find a way to exploit the system. Each layer of the IT defense (firewalls and intrusion detections systems) should increase the risk for the attacker while reducing his chance for being successful while still balance the need that authorized users have for legitimate access to the system. The following figure demonstrates how a layered defense prevents complete system compromise in the event of one layer being violated and stresses the importance of policies, procedures and proper monitoring of the system.

Figure 2. Example of layered defensive measures



(Bednarz, 2007)

It is critical for long term success to maintain balance between the need for security and the need for access by legitimate users. An organization must apply the correct technologies in the proper context of the organization's layered security strategy. The organization must maintain the proper balance of people, operations, and technologies while designing its defense strategy. The entire focus of an organization should be to reduce and mitigate risk of its assets. If a plan involving people and operations is not developed in conjunction with the appropriate technological enablers then failure is eminent and applying the wrong technology or the wrong type of technology to manage risk without involving people and operations will also lead to failure and vulnerabilities in the defense in depth plan.

Critical Incident Response Procedures

A critical incident is any event of a severe nature which threatens to cause, or causes, loss of life, or injury to citizens and/of severe damage to property, and requires extraordinary measures to protect lives. Critical incidents may include explosions, structural failures, fire, or a terrorist incident. In response to a critical incident, the primary function of security personnel is to conduct an orderly evacuation of the facility and facilitate access of first responders. In case of an ongoing incident the Command Center will issue warnings to security personnel and the emergency dispatcher (911) for first responding emergency personnel.

(A) Bomb Threat Procedures

(1) Upon receiving a bomb threat by telephone, the person receiving the threat will; remain calm, activate the trap and trace button on the phone console, begin filling out a bomb threat report form (see example form Appendix C). The call taker will then gather as much information as possible regarding the bomb and its possible location. The call taker will also attempt to listen carefully for any background noise and identifying characteristics of the caller's voice. The call taker will also try to record the exact wording used and gather as much information about the caller as possible. The call taker will also retrieve the suspect's phone number from the trap and trace equipment for investigative purposes and the immediate identification of the caller.

(2) The person receiving/taking the threat information will then contact the Command Center. The call taker will not tell anyone else about the bomb threat.

(3) The Command Center will then obtain the bomb report from the person/ call taker receiving the threat.

(a) The Command Center will then contact the following; Team/Facility General Manager, Director of Facility Operations, Security Manager, the Police Department's Critical Incident Commander, and the Facility Engineer, who will establish a safe meeting place. The Security Manager will then assess the threat and determine whether to initiate/ coordinate a thorough search of the entire facility and grounds.

(b) If the threat does not appear to be a credible threat, the Security Manager will then contact the local police department and make a police report.

(c) If the threat is determined to be credible, the Police Department's Critical Incident Commander will notify the police department. The FBI/ police department's Bomb and Arson section will be notified (Dailey, 2007).

(d) If the decision to evacuate is reached, the Security Manager will notify; the security supervisors, Law Enforcement, and the usher supervisors for an evacuation briefing per the evacuation policy. The security supervisors will then conduct a brief of their staff at the team staging areas. The Security Manager and Law Enforcement Supervisors will coordinate and oversee the evacuation process. The facility personnel will also ensure the security of all facility or team property during and after the evacuation process. The security staff will then secure and open all facility gates prior to the facility announcement to evacuate the facility.

(e) The facility will then be evacuated and upon completion the security staff will then secure the facility, as the facility search is being conducted.

(4) The Police Department's Critical Incident Commander will conduct the threat assessment with the Security Manager and coordinate and direct a search of the facility and grounds. The Incident Commander will also coordinate and liaison between the security staff and the responding police department elements. If the decision to evacuate is made the Law

Enforcement Supervisors will assemble at the designated staging area and direct the evacuation process (Dailey, 2007).

(5) Upon notification of the Team/Facility General Manager, they will have final approval regarding the evacuation of the facility. The Team/Facility General Manager will notify the league of the intent to evacuate. The Team/Facility General Manager will also notify any officials on the playing field/ floor of the decision to suspend play. The Director of Public Relations will then be notified of the decision to evacuate the facility. The Team/Facility General Manager will also have approval authority of over the public address announcement. Upon notification of the Director of Facility Operations, they will notify all employees under Facility Operations of the evacuation. The Director of Facility Operations will oversee the traffic egress process/ evacuation.

(6) The Director of Facility Operations will notify the Director of Ticketing of the decision to evacuate. The Director of Ticketing will then ensure that the vault is closed and secured.

(7) The Facility Engineer will be readily available as a technical resource regarding the evacuation and search of the facility.

(8) The Director of Public Relations will be notified and be available to handle any and all media inquires. The Director of Public Relations will prepare a public address announcement for the evacuation and submit it to the Team/Facility General Manager for approval.

Search Procedures

(9) Upon making the decision to initiate a search of the facility and grounds for an explosive device, the Security Manager will direct the dispatcher to broadcast: “All personnel, there will be a “GREEN TEAM” meeting; please respond to your meeting area” and the Command Center will send out a message to the GREEN TEAM through the IntelliViewer™ wireless network to

their PDA. This announcement will be repeated three times and there will be no further radio transmission. All future communication with supervisors will be made by either Alpha Pager or IntelliViewer™ network. The Command Center will visually clear each section of the Arena using CCTV and wireless cameras to enhance clearing and the evacuation process. Additionally the Command Center will lock down areas that have already been cleared to prevent reentry.

(10) Supervisors will notify the dispatcher by telephone/PDA that they received the message and are enroute to their meeting area. The Command Center will log all calls onto a building search report form. It is necessary for each site to develop a search form that is specific to the facility.

(11) Law Enforcement and facility Fan Assistants (except gate personnel), and Assistant Supervisors will respond to the pre-designated meeting/ roll call areas to form search crews to conduct the search. The team supervisors will arrive at the meeting/ roll call area to conduct a briefing of the search details.

(12) Facility Fan Assistance personnel assigned to the mass crowd gates will unbolt the gates to allow for emergency exit of all patrons. Assistant Supervisors will verify that this has been accomplished and cross-check with other neighboring gates.

(13) Each Security Team will have two, four person search crews. Each search crew will consist of a security supervisor with a PDA connected to the Intelliviewer™ network, or assistant supervisor, a Facility Fan Assistant, and two Law Enforcement Officers familiar with the area. Each crew will deploy and search their assigned area. Upon completion, the Supervisor of each crew will notify the Command Center by PDA that their area is clear.

(14) The Command Center will fill out the building search report form as the Supervisors report in.

(15) If a suspected device is located, the Supervisor of the crew will notify the Command Center by telephone, and the Security Manager will immediately be notified. The Supervisor will then ensure that the area search is completed by additional personnel; checking for possible secondary devices. After a suspected device is located, Supervisors will be given further directions by IntelliViewer™ device. If it is determined that no threat exists, the Security Manager will direct the dispatcher to broadcast; “The GREEN TEAM has concluded its meeting and will resume operations”.

(16) Search Team Assignments

A detailed search team assignment matrix covering all facility areas needs to be developed and assigned to specific search teams.

(17) Security Supervisors/ Assistant Security Supervisors

(a) Form four man teams with Law Enforcement personnel and search your assigned area of the facility. All reports to the Command Center will be made by Intelliviewer™ device. Report any unknown/ suspicious objects or an “Area All Clear”.

(b) Open all mass crowd gates and cross check the mass crowd gates on both sides of your assigned gate to ensure all areas are open. Assist with block points to direct the orderly exit from the facility, and prevent any re-entry of any person to the facility. Organize team members to assist in the guidance of emergency vehicle and personnel to the site area. The perimeter area may increase and there may be a need to move your staff farther away from the facility and the prevention of others from re-entering the facility.

(B) Evacuation

Once the Team/Facility General Manager has given the approval to evacuate the facility, the Security Manager has all supervisory personnel notified by pager/ PDA to respond to the

designated staging area. The Supervisor will assemble all personnel to their “designated” area/roll call area or alternate site. The Security Manager will ensure that roll call is conducted and all facility areas are represented. The Security Manager will then conduct a briefing covering; the nature of the threat, specific instructions regarding the situation. Supervisors will then ensure and give specific instructions regarding the situation to their staff. The Supervisors will then ensure that all areas of responsibility are covered and deploy all personnel to evacuation assignments. The Supervisors will then ensure that the mass crowd gates are open and cross-check the mass crowd gates on both sides of assigned gate to ensure they are open. The Supervisor will then notify the Command Center by IntelliViewer™ device/PDA when all gates are manned and opened.

- (a) Start a verbal evacuation at a central point and work outward.
- (b) Evacuate game personnel from the playing field/facility floor.
- (c) Make evacuation announcement with directions for fans to follow.

Supervisors will ensure that their assigned areas are cleared of all guests, close all perimeter gates and secure from re-entry and verified by the Command Center. Upon completion, report the progress to the Command Center and notify all personnel to respond to their secondary assignment to form an expanding exterior perimeter around the facility.

(C) Mass Casualty Incident

During a mass casualty incident there will be four functions occurring simultaneously at the beginning of the incident. The first is the emergency evacuation of the facility which was previously covered above. The next step is the manning of the Command Center by all GREEN TEAM members; establishing the Command Center as the Emergency Operations Center.

Treatment for the injured by the facility medical staff and first responders and securing an entrance and exit for all first responders (Dailey, 2007).

(1) A detailed plan for the entrance and exit of first responders needs to be developed in order to facilitate a quicker response and needs to be site specific. There is a requirement for a specific route for emergency responders and designated parking area adjacent to the facility which will be controlled/ secured by the security staff.

(2) Emergency procedures for emergency evacuation are the same as the procedures for that of a bomb threat, security staff will direct guests, workers, players, and other facility personnel to the nearest safe emergency exit. The Security Manager will need to coordinate with the police and fire commanders on site for further action to be taken that is specific to the critical incident.

(3) The procedures for establishing the Command Center as the Emergency Operations Center (EOC) is the same as that covered during bomb threat procedures. It is crucial for the EOC to be activated in a timely manner and coordinate response to the critical incident in the most effective manner possible. The Command Center/EOC will be networked with the city's EOC and first responders command post allowing for a fully coordinated response to the incident.

(4) On-site medical treatment will initially be coordinated by the on-site medical personnel. These medical personnel will dictate the closest area suitable for treatment of casualties and establishing a triage system based on the severity of the injuries. Medical personnel will coordinate with the Command Center/EOC and responding medical personnel for the treatment and evacuation of the injured.

(D) Large Crowd Disturbances

Prior to any event at the facility a public safety announcement will be made over the PA system advising guests that for their protection all seating areas will be under surveillance during the event. Wireless cameras can added or moved prior to the event at the facility to provide better coverage based on the event, the floor plan layout, and the amount of guests expected to attend. The Command Center will then have the ability to record from any CCTV camera or wireless camera and transmit the images through the IntelliViewer™ network to the PDA's of the security staff to give them updated, first hand situational awareness. The Command Center will report the size of the disturbance and begin dispatching the Supervisors, security staff and law Enforcement elements to the area. The first Supervisor on the scene will then establish a perimeter to prevent further escalation of the disturbance by additional guests and also determine the number of additional security staff and Law Enforcement required to control the disturbance. Law Enforcement accompanied by the security staff will then enter the area and begin dispersing the people from the area. Security staff should avoid physical confrontation with the combatants to bring the disturbance to a peaceful resolution. If necessary, non-lethal systems, such as pepper spray may be utilized to neutralize the disturbance. The instigating parties should be restrained and removed without delay and taken to a security holding area.

All personnel requiring medical attention will be attended to at this time, prior to being released or removed and transported to the local police department for further resolution. The recordings from the CCTV and wireless cameras will be utilized to determine the instigators of the disturbance and copies will be furnished to Law Enforcement as evidence in criminal proceedings. Additionally, the instigators identified on the recordings will be identified and barred from the facility for any future event and a picture will be maintained in the Command

Center database and this comprehensive list may be accessed over the Intelliviewer™ network by Security Supervisors through the use of their PDA.

(E) Fire Procedures

In the event of a fire, the Command Center will be immediately notified and given the location and size of the fire. The Command Center will then relay the information to the local fire department and the Security Manager. The Command Center will record events and review any previously recorded footage to help determine the origin of the fire. The Security Staff and Law Enforcement will then be dispatched to the area and form a perimeter, removing all guests from the effected areas. Security Staff and Law Enforcement should only attempt to extinguish the fire if it is safe to do so, the type of fire is easily ascertained, and the appropriate fire extinguisher is available. (See Appendix D) If it is too dangerous for the Security Staff to extinguish the fire, the on-site fire department Commander will assume command and take appropriate steps to address the situation. The on-scene Supervisor or Fire Commander may then determine whether evacuation of the facility is necessary. A follow up investigation by the appropriate investigative unit will be conducted with the full cooperation of the facility, in order to swiftly determine the cause of the fire.

(F) Severe Weather

The Security Manager/Command Center is responsible for monitoring the development of any severe weather that may affect the facility and guests. The Command Center/ Security Manager will then advise the Operations Manager/ Director of Operations of any developments in the situation. The Facility Manager will then consult with appropriate league officials or other event officials to determine whether the event should be postponed and evacuation of the facility is necessary. The facility announcer will be directed by the Operations Manager to announce the

postponement of the game/event and the severe weather warning an directions to be followed.

The facility will be evacuated according to the evacuation procedures. Employees will direct guests to appropriate shelter locations and take refuge with the guests until the Command Center instructs or directs otherwise. Supervisors will attempt to gain accountability of those located in their immediate location and report those numbers directly to the Command Center. The on-site Incident Commander will then direct the rescue efforts with all responding emergency service units following the facility Critical Incident Procedures (Dailey, 2007).

(G) Mail and Package Identification and Handling

Some mail or packages may exhibit unique characteristics that are useful in the identification of suspect parcels. All facility personnel who receive and open mail must be knowledgeable about the following warning signs of mail that may pose a potential threat. Protective clothing to include disposable gloves, aprons, and particulate masks are encouraged for personnel who handle large amounts of mail. Characteristics of suspicious mail include:

- Letters that feel rigid, appear uneven or lopsided, lumpy, or are bulkier than normal.
- Letters or packages that are of unusual weight given their size.
- Letters or packages with visible oil stains on the wrappings.
- There is an excessive amount of postage.
- The sender is not identified or there is no return address.
- There is an unusual restricted endorsement is listed such as, “personal”, “private”, or “confidential”.
- Addressee does not normally receive personal mail at the facility.
- Name and title of the addressee are incorrect.
- The city and state postmark does not match the return address.

- The sender has made an attempt to ensure anonymity.
- The mail emits a strange or peculiar odor.
- Package emits a type of noise.
- Mail appears to be opened and re-sealed.
- Handwriting appears distorted or foreign.
- Protruding wires, foils, or strings are visible.
- Pressure or resistance is noted when removing the contents.
- Outer container is irregular or asymmetric and has soft spots or bulges.
- Wrappings exhibits previous use, such as traces of glues, mailing labels, return addresses, or tape.
- Several combinations of tape is used to secure the parcel.
- Unprofessionally wrapped parcel is endorsed “fragile handle with care”, “rush do not delay”, or “open only by_____”.
- Contents of parcel make a sloshing sound or powder is evident.

(www.usps.com/news/2001/press/mailsecurity/pr01_ishandbk.htm).

Handling Suspicious Mail Prior To Opening:

- DO NOT OPEN THE ARTICLE OF MAIL.
- Do Not shake., bump, or sniff the article of mail
- Immediately advise the security staff.
- Isolate the letter or package and secure the area.
- Do Not put the item in water or a confined space, such as a desk drawer or filing cabinet.
- Do Not use a portable radio or cellular phone near the item.

- A danger to further contaminate an area could be increased by opening a window to attempt to vent the area.

Opened Suspicious Mail

- If a package is opened and contains a suspicious substance, chemical, powder, or smell the following steps should be implemented:
 - Isolate the letter or package and secure the area.
 - Notify the security staff and Command Center
 - Do Not open a window or allow anyone else around the letter or parcel.
 - Evacuate the area.
 - Place the parcel in a sealed, plastic bag if possible.
 - Immediately wash hands thoroughly with soap and water without touching the surrounding area.

Handling Player Mail

Due to the possible risks to players/ performers a policy for the segregation of personal and official mail should be developed. The player/ performer mail should be handled separately from the facility mail.

Conclusion

This security plan for the indoor arena captures all the elements necessary to provide a foundation for use and tailoring of the plan to meet the needs of any indoor type facility within the United States. The plan covers: threats to the facility, mitigation steps, defense in depth, and response procedures for critical incidents. Although no plan is 100% fool proof or guaranteed, this plan gives a firm foundation for security personnel to use as a bases for the protection of an indoor facility.

References

Bednarz, Michael A. Master Sergeant, HHC, USDB, (personal communication, March 2007)

Dailey, Tom Major, KCMO Police Department, (personal communication, May 2007)

Davies, S.J., & Minion, R.R. (Ed.). (1999). Security Supervision: Theory and Practice of Asset Protection, 2d Edition. Oxford, UK: Focal Press.

Haddow, G.D., & Bullock, J.A. (Ed.). (2006). Introduction to Emergency Management, 2d Edition. Burlington, MA: Elsevier Butterworth-Heinemann.

Information Assurance Technology Framework, Release 3.1, September 2002, 2-1.

Lardaro, Fred, Executive Director – Business Development, AirVisual Inc.,

(personal communication, May 16,2007)

Krutz, R.L., & Vines, R.D. (Ed.). (2007). The CISSP and CAP Prep Guide, Platinum Edition. Indianapolis, IN: Wiley Publishing Inc.

Wilson, V.T., & Mabery, D.J. (2005). Intelligence in Plain View: Symbols, Logos, Markings, And Non-verbal Clues Suggesting Involvement in Domestic Extremism, Illegal Gangs, And Illegal Drug Activities. Huntsville, TX : Office of International Criminal Justice.

www.adl.org/main_Extremism/peni_california_racist_gang.htm).

www.adl.org/special_reports/wbc/default.asp

www.aijac.org.au/review/2000/258/sounds.html

www.airvisual.com

www.animalliberationfront.com/ALFront/Actions-USA/iowabreakin.htm

www.aoml.noaa.gov/hrd/tcfaq/G1.html

www.cdc.gov/niosh/injury/traumaviol_research.html

www.cnn.com/2006/HEALTH/12/13/e.coli.outbreak/index.html

www.cnn.com/2007/HEALTH/05/17/food.safety.law/index.html

www.cpted-watch.com

www.en.wikipedia.org/wiki/Nazi_Lowriders

www.en.wikipedia.org/wiki/San_Andreas_Fault

www-fars.nhtsa.dot.gov

www.fas.org/irp/crs/RL32521.pdf

www.fbi.gov

www.globalsecurity.org/military/library/policy/army/fm/3-90/ch8.htm

www.hanford.gov/fire/safety/extingrs.htm#fetypes

www.mail-archive.com/islamcity@yahoogroups.com/msg07118.html

www.nizkor.org/hweb/orgs/american/adl/paranoia-as-patriotism/posse-comitatus.html

www.nws.noaa.gov/om/winter/winter1.htm

www.schneier.com/blog/archives/2005/06/white_powder_an.html

www.seton.com/seton/internalHtmlAction.do?relpath=/pages/content/en_US/setonalerts/articles/

0704/0704_dev_securityprog.jsp

www.sportingnews.com/yourturn/viewtopic.php?t=134169

www.sports.espn.go.com/nba/news/story?id=1928540

www.terrorisminfo.mipt.org/pdf/Missouri-Homeland-Security-Strategy.pdf

www.terrorisminfo.mipt.org/pdf/Iowa-Homeland-Security-Strategy.pdf

www.quake.ualr.edu/public/nmfz.htm

www.usps.com/news/2001/press/mailsecurity/pr01_ishandbk.htm

Appendix A : Department of State's list of Foreign Terrorist Organizations

Title 22 of the US Code, Section 2656f, which requires the Department of State to provide an annual report to Congress on terrorism, requires the report to include, inter alia, information on terrorist groups and umbrella groups under which any terrorist group falls, known to be responsible for the kidnapping or death of any US citizen during the preceding five years; groups known to be financed by state sponsors of terrorism about which Congress was notified during the past year in accordance with Section 6(j) of the Export Administration Act; and any other known international terrorist group that the Secretary of State determined should be the subject of the report. The list of designated Foreign Terrorist Organizations (FTOs) below is followed by a list of other selected terrorist groups also deemed of relevance in the global war on terrorism.

Foreign Terrorist Organizations

17 November

Abu Nidal Organization (ANO)

Abu Sayyaf Group (ASG)

Al-Aqsa Martyrs Brigade

Ansar al-Islam (AI)

Armed Islamic Group (GIA)

Asbat al-Ansar

Aum Shinrikyo (Aum)

Basque Fatherland and Liberty (ETA)

Communist Party of Philippines/New People's Army (CPP/NPA)

Continuity Irish Republican Army (CIRA)

Gama'a al-Islamiyya (IG)

HAMAS

Harakat ul-Mujahidin (HUM)

Hizballah

Islamic Movement of Uzbekistan (IMU)

Jaish-e-Mohammed (JEM)

Jemaah Islamiya Organization (JI)

Al-Jihad (AJ)

Kahane Chai (Kach)

Kongra-Gel (KGK)

Lashkar e-Tayyiba (LT)

Lashkar i Jhangvi (LJ)

Liberation Tigers of Tamil Eelam (LTTE)

Libyan Islamic Fighting Group (LIFG)

Mujahedin-e Khalq Organization (MEK)

National Liberation Army (ELN)

Palestine Liberation Front (PLF)

Palestinian Islamic Jihad (PIJ)

Popular Front for the Liberation of Palestine (PFLP)

Popular Front for the Liberation of Palestine-General Command (PFLP-GC)

Al-Qa'ida

Real IRA (RIRA)

Revolutionary Armed Forces of Colombia (FARC)
Revolutionary Nuclei (RN)
Revolutionary People's Liberation Party/Front (DHKP/C)
Salafist Group for Call and Combat (GSPC)
Shining Path (SL)
Tanzim Qa'idat al-Jihad fi Bilad al-Rafidayn (QJBR)
United Self-Defense Forces of Colombia (AUC)

www.state.gov/documents/organization/45323.pdf

Appendix B: Carver Assessment Worksheet Examples

CARVER-H

Indoor Arena Model

Tier I

State/National Single Point of Vulnerable Failure
Critical Government Asset

Tier II

County/Local Critical Asset

CRITICALITY		
CRITERIA	SCALE	
	Tier I	Tier II
Production/supply/service halted for 10 days; Target cannot function without it	17-20	9-10
Production/supply/service halted for 1 week, or 66% curtailment in output, production or service	13-16	7-8
Production/supply/service halted for 1 day or 33% curtailment in output, production, or service	9-12	5-6
Immediate short-term halt in output (less than 24 hours), production, or 10% curtailment in output, production, or service	5-8	3-4
No significant effect on output, production, or service	1-4	1-2
ACCESSIBILITY		
CRITERIA	SCALE	
	Tier I	Tier II
Asset is easily accessible - ineffective or no security measures	17-20	9-10
Asset is located outdoors; Single security perimeter implemented	13-16	7-8
Asset is located outdoors; multiple security measures have been implemented (guards, keys, pinpads, cameras...)	9-12	5-6
Asset is located indoors; A single security measure has been taken	6-8	3-4
Asset is located indoors; Multiple security measures (guards, keys, pinpads, cameras...)	3-5	2
Not accessible or only accessible with extreme difficulty	1-2	1
RECOVERABILITY		
CRITERIA	SCALE	
	Tier I	Tier II
1 month or more to replace, repair, or substitute asset and continue the mission	17-20	9-10
1 week to 1 month replace, repair, or substitute asset and continue the mission	13-16	7-8
72 hours to 1 week to replace, repair, or substitute asset and continue the mission	9-12	5-6
25 to 72 hours to replace, repair, or substitute asset and continue the mission	5-8	3-4

6 to 24 hours to replace, repair, or substitute asset and continue the mission	3-4	2
Less than 6 hours to replace, repair, or substitute asset and continue the mission	1-2	1

CARVER-H

INDOOR ARENA MODEL

VULNERABILITY		
CRITERIA	SCALE	
	Tier I	Tier II
Vulnerable to long-range target designation, small arms, or explosives with a standoff distance of 56 feet**; Computer systems can be hacked into by a novice; Population concentration within the asset is 10,000 or greater or full time staff of 100 or more.	17-20	9-10
Vulnerable to light anti-armor weapons fire or explosives with a standoff distance of 195 feet. Computer systems are protected by a password and firewall, but still can be compromised by a novice; Population concentration within the asset is 5,000-9,999 or full time staff of 25-99	13-16	7-8
Vulnerable to medium anti-armor weapons fire, or explosives with a standoff distance of 260 feet. Intensive prior planning is required to hack into computer system; Population concentration within the asset is 2,500-4,999 or full time staff of 10-24	9-12	5-6
Vulnerable to heavy anti-armor weapons fire, or explosives with a standoff distance of 365 feet. Computer system can only be compromised by an expert; Population concentration within the asset is 500-2,499 or full time staff of 5-9	5-8	3-4
Invulnerable to all but the most extreme targeting measures, or explosives with a standoff distance of 525 feet or more. Computer system is extremely difficult to compromise; Population concentration within the asset is less than 500 or full time staff of 4 or less.	1-4	1-2
EFFECT ON PUBLIC PERCEPTION		
CRITERIA	SCALE	
	Tier I	Tier II
Public views the target as a critical asset and/or key personnel (government, religious) and the compromise/destruction of the asset/personnel creates a widespread panic and has an overwhelmingly negative effect	9-10	4-5
The compromise/destruction of the target/personnel would cause moderately negative effects, consumer confidence lowers, consumption decreases, and there are long run effects	8	2-3
The compromise/destruction of the target/personnel would cause a minor decrease in consumption with no lasting effects in the long run	7	1
Public views the target as having little importance; or they are unaware of the target; the compromise/destruction of this target/personnel will not impede consumption	6	0

** Information regarding standoff distance was figured based on a 1 story unreinforced concrete building with large windows (4' * 5' * 5/32") attacked by a midsized car bomb (220 pounds).

CARVER-H

INDOOR ARENA MODEL

RECOGNIZABILITY		
CRITERIA	SCALE	
	Tier I	Tier II
The target asset or system processes are clearly recognizable from a distance and under all conditions; recognition requires little or no training	17-20	9-10
The target asset or system processes are easily recognizable at small-arms range; recognition requires a small amount of training	13-16	7-8
The target asset or system processes are difficult to recognize at night or in bad weather, or might be confused with other targets or components; recognition requires some training	9-12	5-6
The target asset or system processes are difficult to recognize at night in bad weather, even with in small-arms range; it is easily confused with other targets or components; recognition requires extensive training	5-8	3-4
The target asset or system processes can only be recognized by experts during clear weather conditions	1-4	1-2

HISTORICAL ATTACKS	
CRITERIA	SCALE
Regional multiple attacks on similar target in recent history (past 5 years)	9-10
National multiple attacks on similar target in recent history (past 5 years) (not regionally)	7-8
Regional attack on similar target has occurred in the past 5-10 years	4-6
National attack on similar target has occurred in the past 5-10 years (no regional attacks)	1-3
No similar attacks in recent history	0

CARVER-H

INDOOR ARENA MODEL

Extra Consideration: Explosives

The buffer zone between the asset and the first effective implemented security device can greatly reduce the threat level of critical assets. This zone is important when dealing with explosives.

Questions:

What are the asset's surroundings made of? (i.e.: Concrete building, wooden structure, or a fire walled network) Are the windows or doors shatterproof?

Can a vehicle get inside the buffer zone boundary by way of sidewalk or lawn?

What visual impairments are near the structure to conceal an explosive device (dumpsters, flowerbeds, bushes, etc.)?

Extra Consideration: HAZMAT

Questions:

Are the chemicals properly stored and marked, and what types of containers are dangerous chemicals stored in? How accessible are these containers to outsiders?

Are incompatible chemicals (those that react violently or explode when in contact with each other) stored away from each other?

How accessible are the ventilation systems, are they on the roof or ground level? (If they are on ground level do any fences or structures protect them?)

*How effective is the fence or structure? Wooden fences provide more concealment than chain linked fences.

In the event of an attack: Is there an effective plan for containment, and locations in place for emergency services.

*Locations need to be appropriate for services to access according to Incident Command System.

Extra Consideration: Special Events

The assessment should be completed when the facility is closest to its maximum capacity. Take into consideration: key personnel, religious and ethnic groups, population density, and the special event's duration of time.

MSHARPP & CARVER Modifications:

The Anti Terrorism Assessment Team for the Indoor Arena assessed MSHARPP and CARVER Models for their ability to assess critical assets for the facility. We developed the CARVER-H Model based on combination of both assessment tools. In addition we added a tiered approach in assessing local/county assets (Tier II), and National/State Assets (Tier I). The model is also more accessible to sectors (versus focusing on facilities).

For better Understanding of our Assessment Tool the specific changes are:

1. Accessibility: Reworded to include more detail in security measures.
2. Recoverability: Added the aspect of productivity to the mission, also added more levels based on time requirements for recovery.
3. Vulnerability: Involved more detail on the use of explosive devices, and added computer systems and networks.
4. Effect on Public Perception: Based on panic and consumer confidence in products, and not on populace effects. Includes the importance of the consumers reaction on the economy.
5. Historical Attacks: (Added) Takes into consideration attacks on similar facilities and systems in recent history.
6. Annex: This is a self-awareness of HAZMAT and Explosives. (This tool will help the assessor look critically at the facilities vulnerability to attacks.)

Appendix C: Bomb Threat Report Form

TELEPHONE BOMB THREAT REPORT FORM

INSTRUCTIONS; Be calm. Be courteous. Listen. Do not interrupt the caller. Notify supervisor / Command Centerr of your element by prearranged signal while caller is on the line.

DATE: _____ TIME: _____

Exact words of person placing call: _____

QUESTIONS TO ASK:

1. When is the bomb going to explode? _____

2. Where is the bomb right now? _____

3. What kind of bomb is it? _____

4. What does it look like ? _____

5. What will cause it to explode? _____

6. Why did you place the bomb? _____

7. What is your name and address? _____

Try to determine the following: (circle as appropriate)

Caller's identity: Male Female Adult Juvenile Age _____ years

Voice: Loud Soft High-pitched Deep Intoxicated Other _____

Accent: Local Foreign Region (description) _____

Speech: Fast Slow Distinct Distorted Stutter Slurred Nasal _____

Language: Excellent Good Fair Poor Foul Other _____

Manner: Calm Angry Rational Irrational Coherent Incoherent Deliberate Emotional Righteous

Laughing Intoxicated

Background noise: Office machines Factory machines Bedlam Trains

Animals Music Voices Airplanes Street-Traffic Mixed Party-Atmosphere Other

ADDITIONAL INFORMATION: _____

Appendix D: Classes of Fire Extinguishers

Fire Extinguisher Ratings



Class A Extinguishers will put out fires in ordinary combustibles, such as wood and paper. The numerical rating for this class of fire extinguisher refers to the amount of water the fire extinguisher holds and the amount of fire it will extinguish.



Class B Extinguishers should be used on fires involving flammable liquids, such as grease, gasoline, oil, etc. The numerical rating for this class of fire extinguisher states the approximate number of square feet of a flammable liquid fire that a non-expert person can expect to extinguish.



Class C Extinguishers are suitable for use on electrically energized fires. This class of fire extinguishers does not have a numerical rating. The presence of the letter “C” indicates that the extinguishing agent is non-conductive.



Class D Extinguishers are designed for use on flammable metals and are often specific for the type of metal in question. There is no picture designator for Class D extinguishers. These extinguishers generally have no rating nor are they given a multi-purpose rating for use on other types of fires.



(www.hanford.gov/fire/safety/extingrs.htm#fetypes)