

U.S. Army – Baylor University Graduate Program in Health Care Administration

Hospital Security and Force Protection: A Guide to Ensuring Patient and Employee Safety

A Graduate Management Project Submitted to the Program

Director in Candidacy for the Degree of Master's in Health Administration

April 2006

Captain Jeffery K. Blackwell, CHE

Administrative Resident

Landstuhl Regional Medical Center

Landstuhl, Germany

20071101292

Acknowledgements

First and foremost, I would like to thank my wife and family for their support, which allowed me to spend many hours away from them working on this project. Secondly, I would like to thank my preceptor, Colonel John Collins, for his guidance and mentorship during my residency and specifically on this project. Additionally, it was my pleasure to have the opportunity to speak with and receive guidance from many professionals within the field of security and emergency management. Their comments helped me to develop the Security Assessment Checklist (Appendix B) and the Terrorism Mitigation Matrix (Appendix C). These experts then offered their professional validation of these tools and many provided me with critical analyses to refine them. This completed project has truly been improved through the efforts of the following experts:

Colonel Beverly Pritchett, Deputy Surgeon of the Joint Force Headquarters-National Capitol Region; Joanne McGlown, PhD, MHHA, RN, CHE, Chief Executive Officer of McGlown-Self Consulting, medical consultant with Battle Memorial Institute and adjunct professor at the University of Alabama at Birmingham; Jeff Rubin, PhD, MA, Emergency Manager at Tualatin Valley Oregon Fire and Rescue, member of the State of Oregon's Health Preparedness Advisory Committee, for their guidance and participation with telephonic interviews and suggestions to improve the security tools.

Additionally, the following professionals of Landstuhl Regional Medical Center assisted with evaluation and the application of the security tools to the medical center: Robert Sampe, Emergency Manager; Lieutenant Colonel Carlheinz Stokes, Chief of Environmental Health; Joy DesRosier, CSP, COHN-S, CHMM, MSISM, RN, Patient Safety Program Manager; Major Christopher Gruber, Chief of Operations Division, and Master Sergeant Michael Taylor, Physical

Security Officer. Their comments and suggestions helped create value to the project by the formulation of future security measures at Landstuhl Regional Medical Center in Germany.

Furthermore, members from the Defense Threat Reduction Agency assisted with their vast knowledge of assessing security and force protection at Department of Defense installations by sharing how they conduct assessments. Patrick Kelleher, Terrorist Operations Specialist; Brian Barker, Emergency Management Specialist; Ramesh Sheth, Chief Structural Engineer, and Paul Styer, Infrastructure Engineer; related their experience, which was invaluable in creating the security assessment tool.

Samuel Sherwood, MA, CPM, Senior Consultant at Intergraph Corporation; Raymond Semko, Master Educator for Security Education, Training and Awareness Directorate of the Defense Security Service; Robert Obrien, CHPA, CPS, Provost Marshal for the Southeast Regional Medical Command; James Edward, Provost Marshal for Eisenhower Army Medical Center; each reviewed and validated the Security Assessment Checklist and the Terrorism Mitigation Matrix. Their comments were instrumental in revising the tools.

The help received from these professionals has assisted in creating a tool set for administrators to strengthen security and harden health centers against terrorism. I am very appreciative of everyone's efforts and time spent making this project a success.

Abstract

The purpose of this study was to develop a tool to assess security measures in hospitals and provide an informational tool that would help hospitals address any shortcomings from the security assessment to deter and mitigate the effects of terrorist attacks. This study employed a qualitative approach performed using narrative meta-analysis. This was accomplished by creating a data collection sheet used to highlight salient techniques and categorize each study into three groups: hospital security, terrorism mitigation, and emergency management. No statistical analysis could be performed because of the lack of similar available empirical studies. However, the three categories of literature were used to develop the security assessment checklist, the terrorism mitigation matrix, and provide a summary of emergency management techniques. The security assessment checklist provides hospitals a tool to find vulnerabilities within their security program. Consequently, the findings are then used to mitigate any shortcomings. The terrorism mitigation matrix was created to provide administrators options for implementing terrorism and crime prevention techniques. Pricing information was included to ensure hospitals could implement the maximum amount of terrorism prevention for the least cost. The implementation of these tools will help hospitals become better prepared to prevent terrorist attacks and crime on campus.

Disclaimer

The views expressed in this study are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, Landstuhl Regional Medical Center or the U.S. Government.

Statement of Ethical Conduct in Research

The author declares no conflict of interest or financial incentives in any product or service mentioned in this article. The confidentiality of individuals whose data may have been used in this study was protected at all times and under no circumstances will be discussed or released to outside agencies.

Table of Contents

Introduction	9
<i>Conditions that Prompted the Study</i>	10
<i>Statement of the Problem</i>	11
<i>Research Questions</i>	12
Evolution of Terrorism	12
<i>History of Terrorism</i>	12
<i>Definition of Terrorism</i>	16
<i>Recent Terrorist Attacks</i>	17
<i>Future Concerns</i>	21
Purpose	23
Methods and Procedures	23
Expected Findings and Utility of Results	24
Findings	25
Comprehensive Emergency Management	26
Mitigation Phase	27
<i>Threat Assessment / Hazard Vulnerability Analysis</i>	27
<i>Security Assessment</i>	31
<i>Hazard Management</i>	45
Preparedness Phase	65
<i>Disaster Planning</i>	66
<i>Training</i>	78

<i>Exercises</i>	78
Response Phase	79
Recovery Phase	83
Summary	84
References	87
Appendix A: Chronological Listing of Terrorism Conducted Against Hospitals	95
Appendix B: Security Assessment Checklist	109
Appendix C: Terrorist Mitigation Matrix	122
Appendix D: Resources and Websites	129
Appendix E: Security Assessment and Recommendations for LRMC	136

List of Figures

i. Figure 1. Trending of international terrorist attacks 1983 – 2004	16
ii. Figure 2. Trending of casualties from International terrorist attacks for years 1983 – 2003	17
iii. Figure 3. Type of terrorist act in the U.S. for years 1980 – 2001	18
iv. Figure 4. Location of terrorist activity in the U.S. for years 1980 – 2001	19
v. Figure 5. The four phases of comprehensive emergency management	25
vi. Figure 6. Kaiser Permanente HVA tool	28
vii. Figure 7. Protecting outdoor air intakes	58
viii. Figure 8. Surface technology for immune building environment	59
ix. Figure 9. Vehicle checkpoint design	60
x. Figure 10. DOD standoff distance for new construction	61
xi. Figure 11. JCAHO emergency management checklist	66
xii. Figure 12. Levels of PPE	71
xiii. Figure 13. OSHA's minimum PPE for hospital-based first receivers	73
xiv. Figure 14. Healthcare facility response plan for chemical or biological weapons release	80

Hospital Security and Force Protection: A Guide to Ensuring Patient and Employee Safety

Introduction

Landstuhl Regional Medical Center (LRMC) serves as the primary treatment facility for injured Soldiers being treated from wounds received during Operation Iraqi Freedom (OIF), Operation Enduring Freedom (OEF), and the Global War on Terrorism (GWOT). Landstuhl is located in Southwest Germany in the forest state of Rhineland-Pfalz and has played a major role in the treatment of casualties since its dedication in 1953. Additionally, LRMC has been instrumental in responding to acts of terrorism by treating the injured of the 1980 aborted rescue attempt of American Hostages in Iran, the 1983 U.S. Marine Corps Barracks bombing in Beirut, the 1986 LaBelle Disco bombing in Berlin, the 1994 Sarajevo marketplace bombing, the 1998 U.S. Embassy bombing in Nairobi, and the 2000 bombing of the U.S.S. Cole (LRMC History, 2005). Subsequently, LRMC is viewed as the hub of American Medicine in Europe and stands as an icon of the United States Military worldwide.

An emerging tactic used by terrorists is the targeting of hospitals as a primary or secondary objective. Incidents have sharply increased since the tragic attack on the World Trade Center in 2001 (See Appendix A). This new security threat coupled with the prestige that is associated with LRMC created legitimate concerns for the safety of patients and employees in the facility. Upon review of Landstuhl's Emergency Management Plan and security initiatives, LRMC is revising policies and procedures and making changes to infrastructure to decrease the threat of terrorist attacks aimed at the Hospital.

Similarly, all hospitals are a target for terrorism. However, the threat may not be equally distributed. The likelihood for a rural hospital to fall prey to a terrorist attack is not as high as a

hospital located in close proximity to large cities and sites of national interest. Nevertheless, all hospitals need to be prepared to react to local emergencies whether they are terrorist incidents, natural disasters, hazardous material accidents, flu pandemics, epidemics, or acts of workplace violence. Furthermore, all healthcare facilities accredited by the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) are required to maintain an “all-hazards” approach to emergency management (Joint Commission Resources, Inc., 2005). Developing and implementing the “all-hazards” plan is tremendous work and requires hospitals to address issues for which they may have not been previously prepared.

Therefore, to decrease the workload for healthcare facilities, the purpose of this study is to develop a tool to assess security measures in all hospitals and provide information that will help hospitals address any shortcomings derived from the security assessment to deter and mitigate the effects of terrorist attacks. Additionally, the author will apply these tools to Landstuhl Regional Medical Center and provide a report of shortcomings including possible solutions to the Hospital Commander.

Conditions which prompted the study

The conditions prompting this study are twofold. First, in July 2005 Landstuhl was notified of intelligence reports, which designated the hospital as a potential target for terrorist attacks. This information prompted the execution of a security assessment, which revealed several vulnerabilities that needed to be addressed. At that time, it was deemed necessary to update and make changes to the security plan, Emergency Management Plan (EMP), and the Force Protection plan. Additionally, there are many terrorist cells operating in Germany and Europe. This fact became quite evident to Great Britain, who recently fell subject to attacks on their mass-transit systems by Al-Qaeda. Many of the terrorists involved were not British

nationals but foreigners with ties to other European countries. Currently, there are 10 known terrorist groups operating in Germany to include Al-Qaeda (Terrorism Research Center, 2005).

The second condition prompting the study is the worldwide increase in attacks against hospitals over the last five years. These heinous attacks have been largely the result of extremist terrorist groups such as Al-Qaeda, Hamas, and the Palestinian Liberation Organization (PLO), who claim a holy war or Jihad to justify their deeds. Thus, the threat of becoming a target of terrorism that LRMC faces similarly applies to most urban, military, and historic hospitals in the United States.

Statement of the Problem

Although terrorism has existed for centuries, its effects have been local and minimized until the adoption of chemical, biological, radiological, nuclear, and explosive weapons (CBRNE). The introduction and use of these weapons for terrorism increased steadily from the latter half of the twentieth century until the historic and catastrophic terrorist attack by Al-Qaeda on September 11, 2001. Since then, terrorist attacks have increased in severity and frequency worldwide by more than 35% (Committee on Government Reform, 2004). In the midst of this period of unrest, hospitals continue to be plagued by violence towards medical staff, which most often occurs at the emergency department. "According to the National Institute of Occupational Safety and Health, hospital workers experienced assaults at a rate of 8.3 per 10,000 employees in 1999, more than quadruple the two assaults per 10,000 employees in other sectors" (Shinkman, 2003, p. 10). The compounding effect of these issues causes great stress on hospitals to prepare to treat mass casualties from terrorist incidents, as well as, mitigate the threat of violence and terrorism directed against them.

Research Questions

- How do hospitals prepare for mass casualty events?
- What hospitals are at risk for terrorist attacks?
- What can hospitals do to protect themselves from terrorist acts?
- What process or steps can hospitals take to analyze their own security deficiencies?
- How much should security and force protection for hospitals cost?

Evolution of Terrorism

History of Terrorism

The ability to understand and combat terrorism lies in its foundation and history. It is therefore necessary to discuss the origins and evolution of terrorism from its earliest history to the current atrocities experienced today. This history can be systematically broken down into distinct periods where ideologies differed in the terrorist's scheme. Some of these periods may overlap, especially during the transition from one phase to the next.

In the first period, religious based terrorism erupted during 66 – 72 A.D., when Jewish zealots targeted Roman property and soldiers in an attempt to rid their occupation of Palestine. One Jewish terrorist group during this era was called the Sicari, who murdered other Jews that fell away from their faith (About, Inc., 2005). Furthermore, the history of terrorism between the Shiite and the Sunni Muslims traces its origins back to the Medieval Christian era (1090-1291), in which a Shiite sect called the “hashashins” enacted terror on the Sunni's by murdering without distinction, even women and children. The term assassin is derived from the word “hashashin”. They believed they would receive a martyr's paradise if they were killed. In other words, they would receive 72 virgins and achieve paradise in the afterlife (State of Delaware, 2005).

The second period details the birth of modern terrorism in the 18th century during the French Revolution, when Maximillian Robespierre ordered the deaths of those who opposed him. Over 40,000 people were killed by the guillotine and it was at this time that the word “terrorism” was coined due to Robespierre’s reign of terror. This was the first time a ruling government would sponsor terrorism (About, Inc., 2005).

Later, terrorism would evolve from being sponsored by the government to terrorists attacking and striking terror in the government. This was known as the anarchist period. It was during this time that President William McKinley was killed by Leon Czolgosz, an anarchist with hatred for the American government, who was linked to leaders of the anarchist movement. This act coupled with the assassination of Archduke Franz Ferdinand led to the start of the First World War (Nash, 1998). It was also during this period that anarchists first understood terrorism could be used as a tool of communication. In general, if anarchists assassinated a noble or set off a bomb, then people would ask why and be ready to listen. This concern by society has led to the success of terrorism, because the message, which the terrorists wanted to present, consumes a captive audience leading to the concept of “propaganda by deeds” (State of Delaware, 2005). After listening to the terrorists’ propaganda, many in society became sympathetic with their goals, which lead to the further success of terrorism.

This newly discovered communication tool proved especially successful during the next period. Shortly after the beginning of World War I, another period of terrorism emerged called “anti-colonial terrorism”, which lasted until 1965. During this period, terrorists from colonized countries fought against the superpowers of France and Britain to gain independent, self-ruling governments. President Woodrow Wilson further complicated the matter by stating in his famous Fourteen Points, that colonial claims should be adjusted and the inhabitants should be

allowed to govern themselves. After the close of the First World War and the exit of the United States from world politics, France and Britain divided the defeated German, Austrian, and Ottoman empires between themselves. This included Egypt and the Gulf States of Iraq, Palestine, and Jordan, which fell to Britain to manage. This division coupled with President Wilson's previous statement of encouraging independent rule and the advance in weaponry from the war provided all the ingredients to refuel terrorism in a "post-colonial" era (Shughart II, William F., 2005).

An example of "anti-colonial terrorism" occurred during the Irish Rebellion (1919 - 1921), when the Irish desired to gain independence from Britain. Several key developments transpired during the rebellion, which altered terrorism as we know it today. The first development was the idea of selective terrorism, which is the targeting of particular individuals. In the case of the Irish Rebellion, those targeted were government officials, police, military, and judges. Secondly, the implementation of cell operations took place. Cells were used to distribute command and control to small entities that could then coordinate with other cells for larger attacks. Finally, the idea of sustained operations emerged. Continuing the attacks over a long period allowed support to grow for the terrorist cause and demoralized the colonial rulers. These tactics were successful for the Irish and several others as they gained their independence and became independent states (State of Delaware, 2005). This new wave of terrorism proved to the world that terrorist activities could bring about change.

At the beginning of the "post-colonial" era, violence broke out in Egypt and eventually engulfed the Middle East. In 1954, the Algerian Civil War, conducted by the Front de Liberation Nationale (F.L.N.), began as a non-lethal campaign targeting French government offices and buildings. However, with little progress made in achieving their goal, the strategy changed to

mass urban terror. The F.L.N. began bombing multiple civilian targets and terrorists gunned down 49 European civilians. The terrorist attacks culminated with the assassination of the French Mayor of Algiers. This caused anti-Muslim rioting and escalating violence on both sides. The F.L.N. attacks finally subsided with counterterrorism techniques by the French, which included torturing terrorists in order to gain intelligence. However, it did not work. Eventually, Algeria gained its independence by using a small number of terrorists to target French interests, which weakened France's will to occupy the region. Terrorist attacks continued throughout the colonial ruled territories, with increasing frequency and severity, which lead to independence for Israel and Cyprus as well (Shughart II, William F., 2005).

During the Vietnam War, left-wing terrorism emerged in a new period of violence. Opposition to the war throughout the world fueled extreme left-wing groups, which assisted the Palestinian Liberation Organization (PLO) in the United States, Latin America, and Europe. The PLO directed assassinations, kidnappings, and bombing campaigns to further their political and social agendas, which were in opposition to the United States and its Allies. In Germany, the Red Army Faction (RAF) with ties to the PLO bombed the US Fifth Army Corps officer's mess in Frankfurt. In the United States, groups such as the Black Panthers, Symbionese Liberation Army (SLA), the Weathermen, and the Students for a Democratic Society (SDS), were responsible for bombings, kidnappings, and murder generally associated with an anti-imperialist agenda. These types of groups were active through the 80's delivering their ideologist views in the form of terrorist acts (Shughart II, William F., 2005).

The final period of terrorism has been characterized as a return to religious ideology, which calls for the destruction of anyone who opposes the religious extremist. This religious period of terrorism, which began during the Afghan War (1979 – 1989) is primarily due to

militant Islamists. The war was subsidized by the United States on one side and the former Soviet Union on the other. The U.S. gave modern weapons to Afghans who otherwise would not have had access to them. The war also gave prominence to individuals like Osama Bin Laden, who became a leader and set up training camps for his recruits. Through these experiences, Osama Bin Laden was able to obtain money, weapons, and develop connections that would enable him to set up the Al-Qaeda network (Lee, R., 2006). Al-Qaeda is now a household name due to the unexpected attacks of September 11, 2001, when the terrorist network hi-jacked four airplanes and successfully flew them into the World Trade Center in New York, City, the Pentagon in Washington D.C., and crashed one in Pennsylvania overall killing more than 3,000 people. This continues today with the War on Terror, Operation Enduring Freedom, and Operation Iraqi Freedom.

Definition of Terrorism

It is necessary to define terrorism in order to conduct a research study, so that the reader will understand the criteria for choosing which are to be considered terrorist attacks. Exploring the history of terrorism enables one to see its evolution from the beginning to present. Because terrorism has encompassed religious, political, and social ideologies, and continues to change, it becomes difficult to define. Additionally, there exists no universally accepted definition of terrorism. However, by reviewing seven current definitions of terrorism, several general themes emerged. First and foremost, terrorism is a premeditated and unlawful violent act. Secondly, terrorist acts are motivated by ideological, political, or religious purposes. Finally, the target of terrorism, unlike conventional war, is the innocent such as civilians instead of enemy combatants (i.e. soldiers of the opposing armed forces). Stress should be placed on “combatant” because soldiers performing medical and chaplain roles and not engaged in offensive military situations

should still be considered innocent. Thus, I propose the use of the following more comprehensive definition of terrorism:

Terrorism is any political, religious, or ideologically motivated unlawful violent act or threat perpetuated against innocents and public or private property for the purposes of intimidation, coercion or to compel a government to abstain from performing any act.

This definition will be used to determine whether events are considered terrorist acts.

There is less controversy over the terms used to describe domestic and international terrorism: Therefore, the definitions of the Federal Bureau of Investigation (FBI) will be used. Essentially, domestic terrorism includes those activities carried out against a government or people without foreign influence, while international terrorism involves activities that are directed by foreign influence (FEMA, n.d.). Furthermore, the U.S. Department of State (2004), considers an International terrorism incident significant if, “it results in loss of life or serious injury to persons, major property damage, and/or is an act or attempted act that could reasonably be expected to create the conditions noted” (p. 95). Understanding the terms associated with terrorism and determining which definitions will be used minimizes confusion and discrepancies in this and future studies.

Recent Terrorist Attacks

Data from the U.S. Department of State’s publications, *Patterns of Global Terrorism* (1983 – 2003), *Country Reports on Terrorism* (2004), the FBI’s annual report, *Terrorism in the United States* (1999 – 2001), and the National Counterterrorism Center report, *A Chronology of Significant International Terrorism for 2004*, were compiled to present the terrorist activity directed at the United States and compared to worldwide incidents. Trend lines were added to illustrate current activity (See Figure 1).

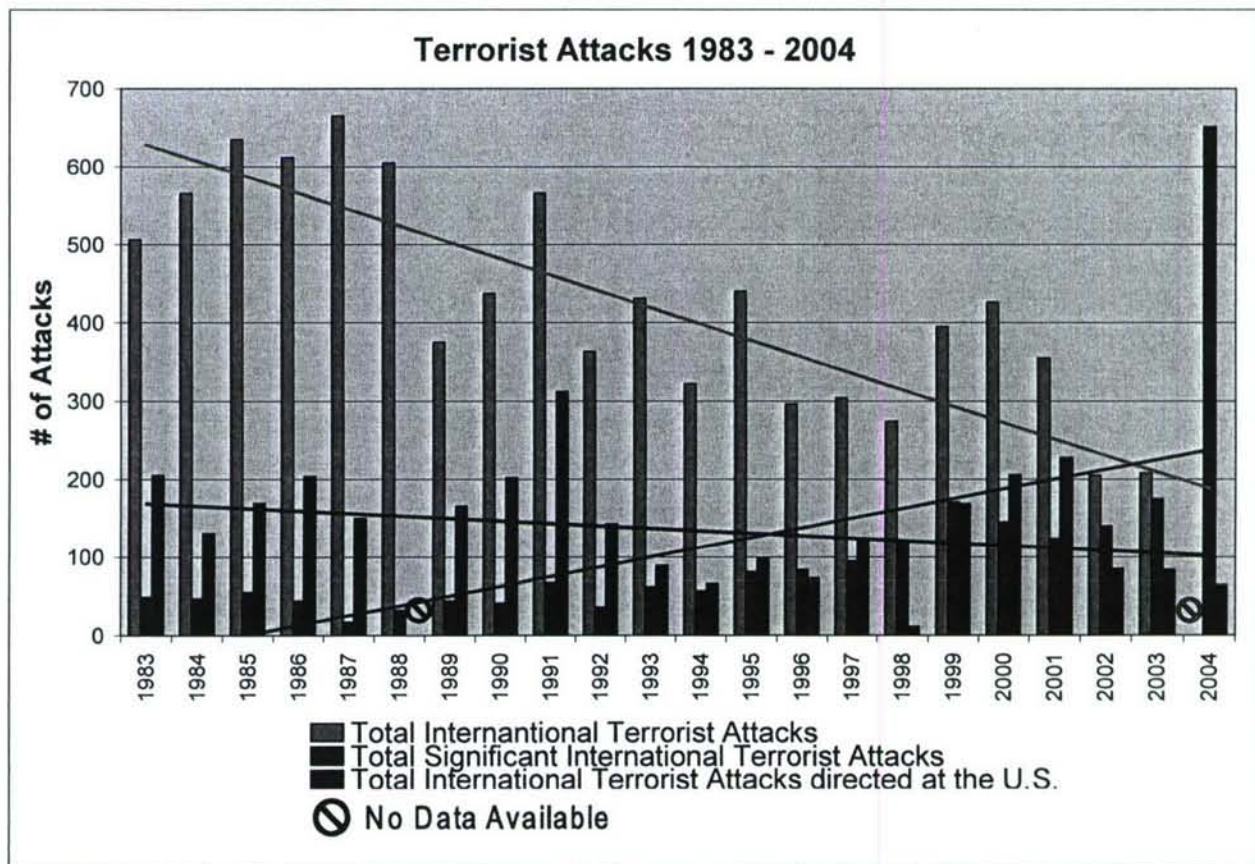


Figure 1. Trending of international terrorist attacks 1983- 2004.

Figure 1. illustrates the total number of international terrorist attacks and the total number of attacks directed at the U.S. to be declining. This is especially true for the years 2002 – 2003. These were also the first years of the Global War on Terrorism (GWOT) when OEF and OIF began, which may have had an initially significant effect by disrupting Al-Qaeda and other terrorist networks. However, the 2004 data for total international terrorist attacks is missing and must equal or exceed the total number of significant international terrorist attacks. Thus, even

with the decline, 2004 would likely show the largest number of attacks in over 20 years.

Likewise, the total number of significant International terrorist attacks has more than tripled from previous years. The increase in attacks may signify a regrouping of international terrorist cells and shift from the current trend of attacks. These numbers indicate that even though the total number of attacks are declining, the magnitude and devastation associated with the attacks is rising. This conclusion was derived using the previously mentioned definitions of terrorism.

Correspondingly, Figure 2. illustrates that the number of casualties is climbing, indicating that even though there are fewer acts of terrorism, the ones that occur are more deadly.

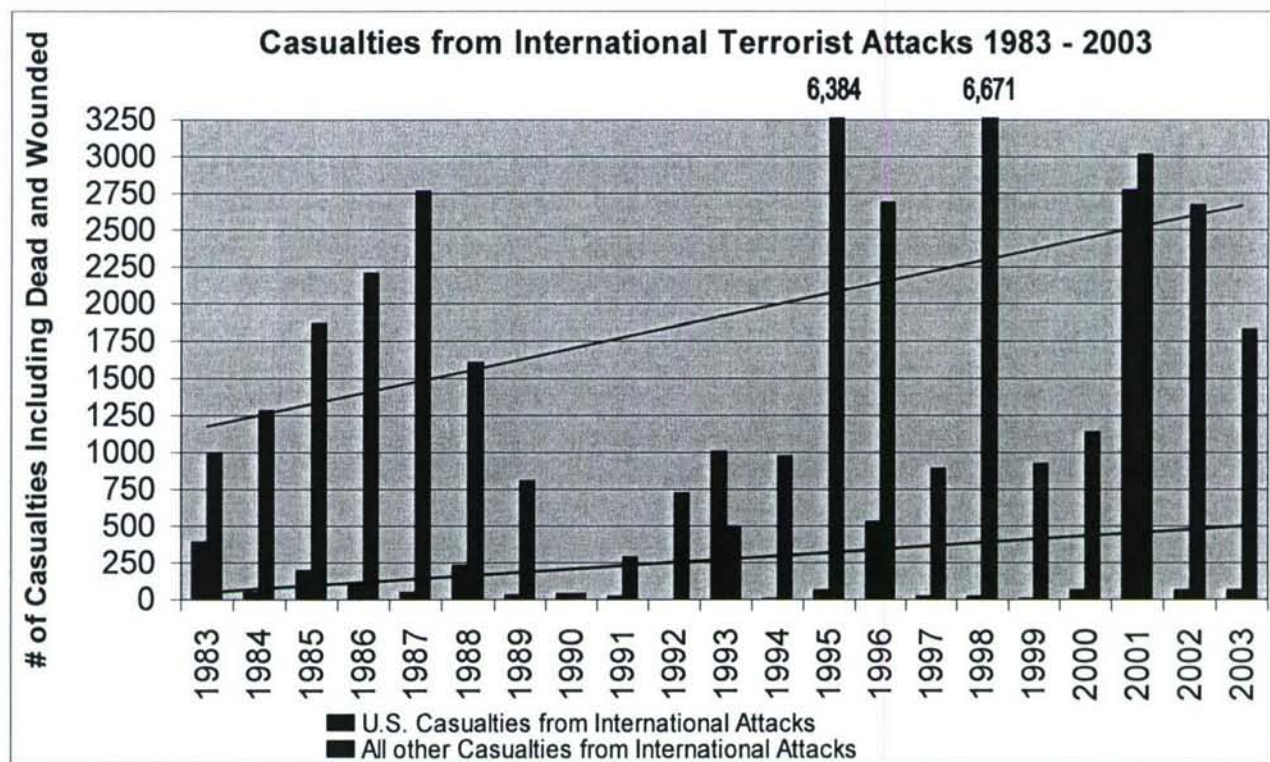


Figure 2. Trending of casualties from International terrorist attacks for years 1983-2003.

A review of the U.S. terrorism data provided by the FBI outlines the type of terrorist attacks, which either have occurred or were prevented from the years 1980 – 2001 (See figure 3.).

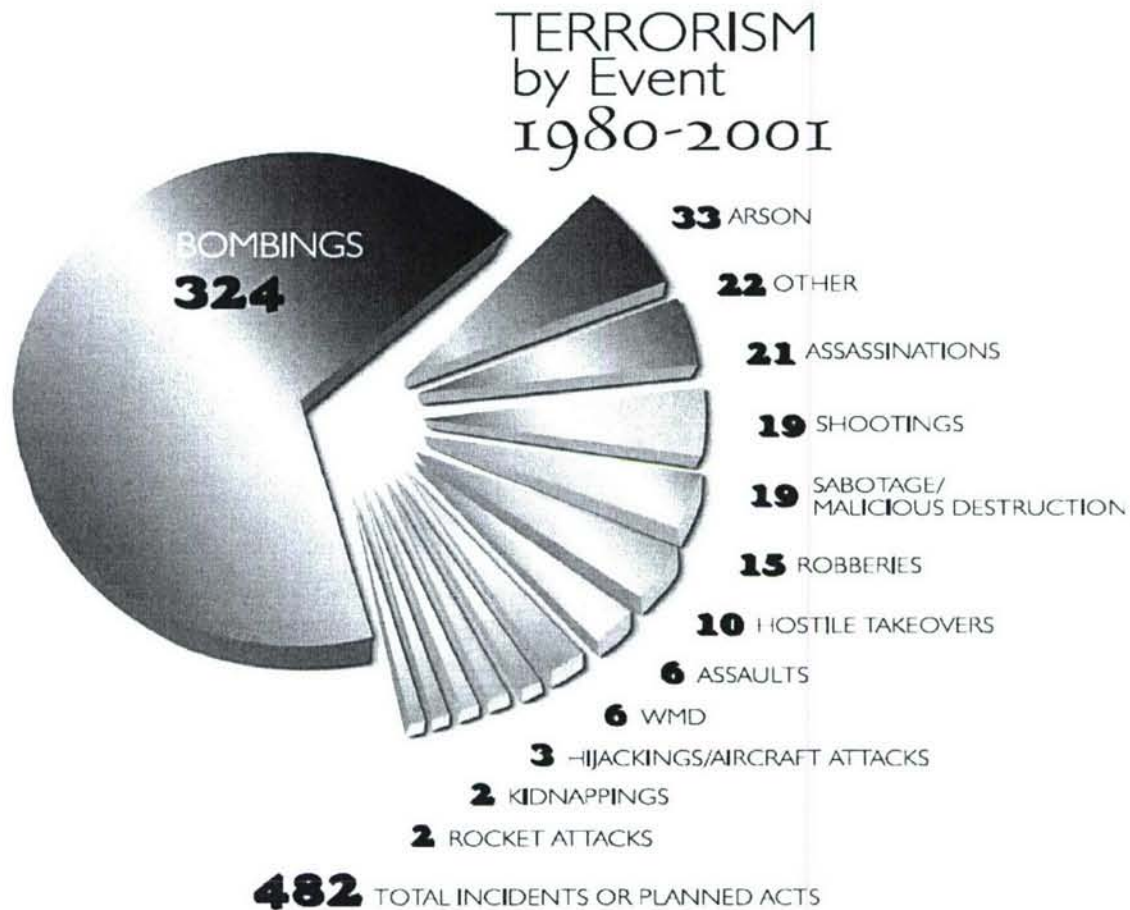


Figure 3. Type of terrorist act in the U.S. for years 1980 – 2001 from the U.S. Department of Justice FBI's annual report on terrorism 2000/2001 (2002).

In this figure, 75% of the planned or executed attacks were bombings. This statistical significance should help us prepare for future attacks. Specifically, businesses within the U.S. should be more concerned about how to prepare for a bomb attack. Moreover, investigating the frequency of attacks by region would enable us to predict the level of threat and possible future terrorist activity for those areas (See figure 4.).

TERRORIST ACTIVITY_{by} REGION 1980-2001

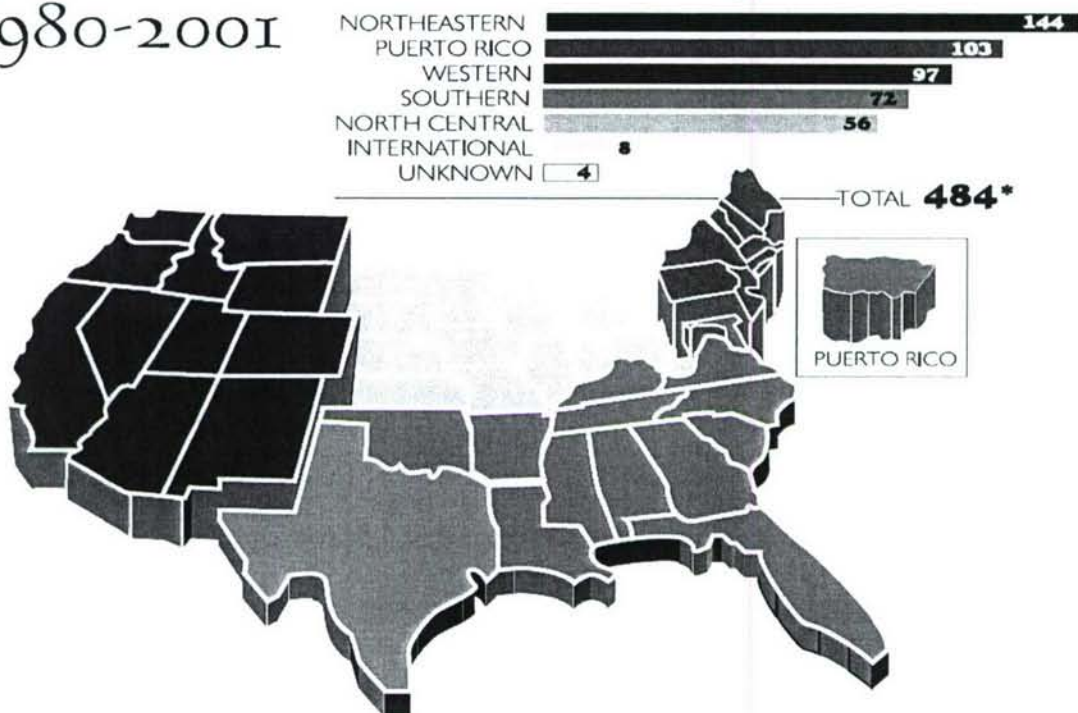


Figure 4. Location of terrorist activity in the U.S. for years 1980-2001 from the U.S. Department of Justice FBI's annual report on terrorism 2000/2001 (2002).

The available terrorist data for the United States indicates that Northeastern states may have twice the risk of terrorist bombings than the North Central states. Therefore, an awareness of the history of terrorism and of terrorist activity trends enables one to perform adequate threat assessments and implement measures for the most likely terrorist events.

Future Concerns

The past 25 years of terrorist attacks have primarily been carried out with the use of conventional weapons such as explosives and small arms. This is supported by figure 3, which suggests that conventional weapons are used in almost all terrorist attacks. High-tech weapons are generally more expensive, harder to obtain, require sophisticated training, and do not always have an immediate effect. However, the use of high-tech weapons such as anthrax powder, sarin

gas, and nuclear devices elicit a tremendous amount of fear from the public. This fact alone increases the potential for greater use by terrorist groups. Consequently, the likelihood that future terrorist attacks will use high-tech weapons increases with advances in technology. For this reason, hospitals need to be prepared to react to these types of attacks.

Another concern is the recent targeting of hospitals for terrorist attacks (See Appendix A). This listing of terrorist events covers a few terrorist attacks targeting hospitals over the last five years. This should not be considered a comprehensive list of all hospital attacks, but should provide examples of specific tactics employed against hospitals. The development of Appendix A consisted of numerous internet searches and six terrorist timelines to compile the information, which necessitated its own list of references. Prior to 2001, there were less than three International attacks identified against hospitals as compared to 14 in 2005 alone.

In June of 2005 The Washington Times reported, “an FBI affidavit said Hamid Hayat admitted attending an Al Qaeda training camp in 2003 and 2004, and the trainees were being taught to target hospitals and large food stores in the United States” (Seper, J., 2005). Additionally, late in 2004, the FBI released a report that Veterans Affairs (VA) hospitals may be a specific target for terrorism due to their affiliation with the military. Since they are located off military installations, they become an easier target (Associated Press, 2004). Further evidence strengthening the argument that terrorists are targeting hospitals emerged in April of 2005, when unknown assailants impersonated JCAHO inspectors claiming they were performing unannounced inspections in Boston, Detroit, and Los Angeles. In all cases, the impersonators either left or were expelled when security or staff questioned them about their identity. No plots were uncovered, but it may have been a tactic to uncover weaknesses and collect information (Brown, D., 2005). All of these events coupled with the recent terrorist attacks targeting hospitals

suggest that even though most of the events have been overseas, the U.S. will likely become a victim of terrorist activity of this nature in the future.

Purpose

The purpose of this study is to develop a tool to assess security measures in all hospitals and provide an informational tool that will help hospitals address any shortcomings from the security assessment to deter and mitigate the effects of terrorist attacks. Additionally, these tools will be applied to Landstuhl Regional Medical Center and will provide a report of shortcomings to include possible solutions to the Hospital Commander.

Methods and Procedures

This study employed a qualitative approach performed using narrative meta-analysis. Gene V. Glass (1976) presented the meta-analysis as an alternative to the traditional narrative review and described it as:

the analysis of analyses...the statistical analysis of a large collection of analysis results from individual studies for the purpose of integrating findings. It connotes a rigorous alternative to the casual, narrative discussions of research studies which typify our attempts to make sense of the rapidly expanding literature (p. 3).

The basic premise for this research design involves combining findings of individual studies to provide a more comprehensive analysis of the subject. This was accomplished by creating a data collection sheet, which was used to highlight salient techniques and categorize each study into three groups: hospital security, terrorism mitigation, and emergency management. When completed, the five proposed research questions were juxtaposed with the techniques from the three categories to determine what aspects of each could be used for comparison and what statistical analysis, if any, could be performed through the narrative meta-analysis. It was

determined that because of the lack of similar empirical studies available, no meaningful statistical analysis could be performed. However, the three categories of literature were used to develop the security assessment checklist (Appendix B), the terrorism threat mitigation matrix (Appendix C), and provide a summary of emergency management techniques.

Consequently, the developed tools and synthesized emergency management summary was successful in answering the proposed research questions. The success of which, was determined by the validation of 16 professionals within the field of study (See Acknowledgements). Their comments and suggestions were used to modify the tools, thus, minimizing any shortcomings. These tools may be used as the basis for a process to ensure hospitals maximize their efforts in assessing and implementing security and force protection measures.

Additionally, an approximate cost for each terrorism mitigation technique was determined to allow for a comprehensive analysis. This presents viable options coupled with financial information about which techniques are more attainable. This will allow hospitals to assess their threats and implement the most cost effective means for lessening the effects of a terrorist act.

Expected Findings and Utility of Results

The findings should show that most facilities are ill prepared for terrorist attacks and that by utilizing the proposed tools for assessing and implementing security and terrorism mitigation measures, their hospital will become hardened against them. The utility of results has the potential to create a single source for information and provide tools to serve as a basis for evaluating and implementing security and force protection at medical facilities.

Findings

The findings were consistent with the expectations showing hospitals are not prepared for terrorist attacks. A GAO report entitled, *Hospital Preparedness: Most Urban Hospitals Have Emergency Plans but Lack Certain Capacities for Bioterrorism Response* (2003), found that most hospitals did not have the surge capacity or equipment to treat a large influx of patients characteristic of a bioterrorist attack. Additionally, less than half of hospitals had even held drills incorporating bioterrorism scenarios. Even though the focus was on bioterrorism, a large influx of patients could occur with any type of terrorist attack or epidemic. Tara J. O'Toole, M.D., M.P.H., of Johns Hopkins Center for Civilian Biodefense Studies, stated, "Few, if any, hospitals in America today could handle 100 patients suddenly demanding care. There is no metropolitan area, no geographically contiguous area, that could handle 1,000 people suddenly needing advanced medical care in this country right now" (Joint Commission Resources, 2006, p. 1). Furthermore, common deficits in hospital preparedness and emergency response are communication, disease identification, laboratory capability, sufficient Personal Protective Equipment (PPE), hospital security, decontamination facilities, medical / pharmaceutical supplies, training, and adequate disaster or terrorism response drills (Rubin, 2004).

Furthermore, the literature review should be viewed as a short synopsis of a "How To" guide for emergency management. However, this should not be considered an exhaustive report on the subject. The remaining findings and tools are contained within the next section entitled Comprehensive Emergency Management. It was determined that the provision of information within the current JCAHO structure for emergency management planning would be beneficial for the evaluation and development of a hospital's security and emergency management plans.

The developed security assessment checklist, terrorism mitigation matrix, and resources are tools to assist an organization in achieving a “Hardened” state in response to terrorism and other perceived threats with a minimal amount of research and effort. The former Director of Homeland Security, Tom Ridge, stated to the AHA:

If we are to secure our homeland ...our hometowns must be secure. The critical role you play in that effort cannot be underestimated. The President’s executive order directed our office to develop and coordinate a comprehensive national strategy to secure the United States from terrorist threats or attacks. We must protect our borders, our people, our physical and electronic infrastructure, our schools and businesses and, yes, our hospitals (2002).

As leaders and administrators in the healthcare field, we have a duty to protect our patients and ensure the safety of our staff. The time has come to make changes in our processes and increase the security posture of our hospitals. The true results of this study will ultimately depend upon the dissemination and use of information by healthcare facilities.

Comprehensive Emergency Management

Comprehensive Emergency Management is a concept, which guides entities through the assessment of threats facing organizations through preparation, mitigation, and response activities. Figure 5 illustrates the Life Cycle of comprehensive emergency management.

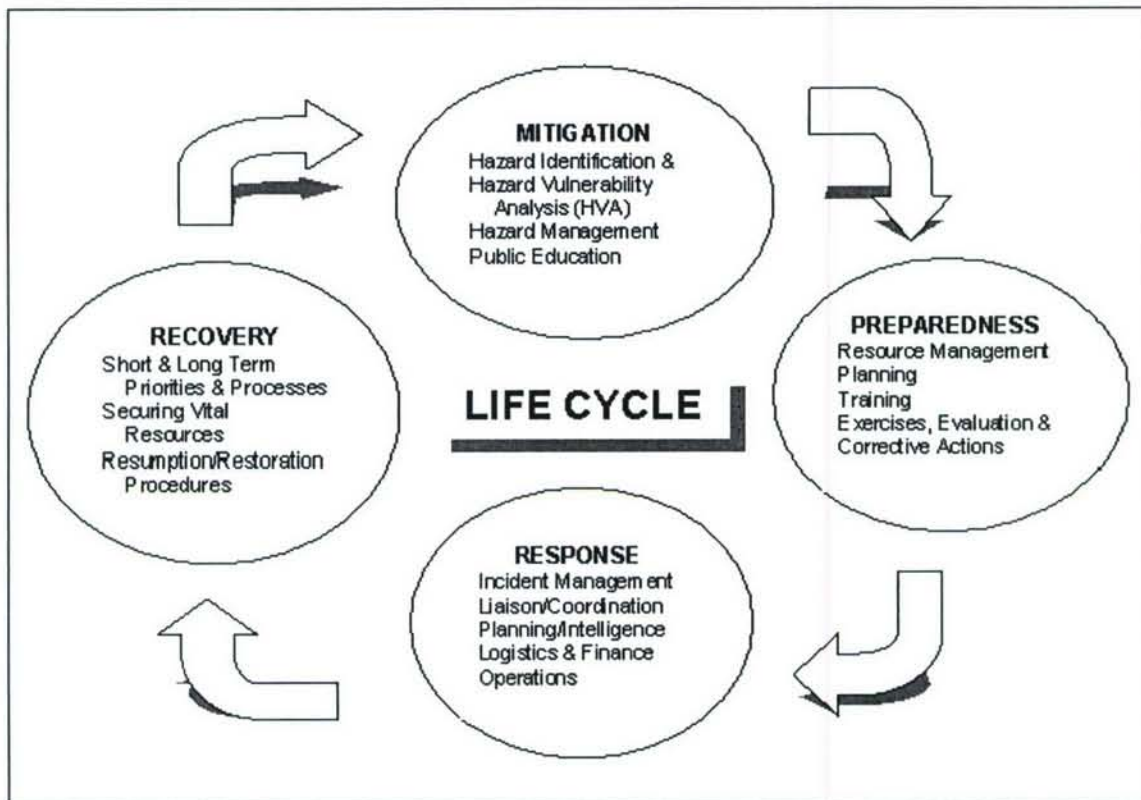


Figure 5. The Four Phases of Comprehensive Emergency Management from the Department of Veterans Affairs website (2006).

Essentially, these four phases represent a risk management program which provides the ability to respond to natural disasters, technology emergencies, security, and terrorism. Each phase will be discussed. However, the focus will be on hospital security and terrorism mitigation. Subjects may be discussed in more than one phase to ensure the continuity of security measures or terrorism mitigation within the life cycle of emergency management. This broad-spectrum program may be tailored to any business or facility when following its basic principles and procedures.

Mitigation Phase

Threat Assessment / Hazard Vulnerability Analysis

Jerry Mothershead (2004), a consultant for the Navy Medicine Office of Homeland Security, states the two essential components of risk management are threat assessments and

hazard vulnerability analyses (HVA). Threat assessments involve determining how probable events (terrorism, natural disaster, etc) are likely to occur. In regards to terrorism, the Department of Defense defines threat assessment as the process to conduct a threat analysis or:

A continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups that could target the DOD Components or the DOD Elements and Personnel. A threat analysis shall review the factors of a terrorist group's existence, capability, intentions, history, and targeting, as well as the security environment within which friendly forces operate. Threat analysis is an essential step in identifying probability of terrorist attack and the results in a threat assessment (DODD 2000.12, p. 34).

The threat analysis can easily be adapted for natural disasters, researching the type and frequency of events on record to determine the probability of an act occurring. Identifying possible threats facing your hospital or facility is only the first portion of risk management.

A more comprehensive analysis within the mitigation phase of emergency preparedness is the HVA, the second essential component of risk management. The Hazard Vulnerability Analysis combines the threat assessment with how the event would subsequently impact business, property, and personnel, as well as, taking into account how well the organization is prepared to react to the specified threat. The Joint Commission on Accreditation of Healthcare Organizations requires that hospitals address the four phases of emergency management as they relate to an all hazards disaster plan and conduct an HVA to determine threats and vulnerabilities to the facility (Steinhauer & Bauer, 2002). As with most JCAHO requirements, there is no specific HVA tool that hospitals are mandated to use. JCAHO only requires that facilities must assess the risks and vulnerabilities of the facility and have plans to mitigate them.

There are many HVA's from which to choose. Some have scoring systems and some just ensure you address how to respond to risks or hazards facing the facility. The American Hospital Association (AHA) in conjunction with the American Society of Healthcare Engineers (ASHE) developed a HVA tool that may be purchased for a small fee and can be found at www.ashe.org. Another HVA tool developed by Kaiser Permanente (See Figure 6) was praised as a best practice in OSHA's Best Practice for Hospitals-Based First Receivers of Victims publication (2005) and can be downloaded for use at www.healthcarefreeware.com/hlt_ha_an.htm. Figure 6 shows the natural hazards matrix and the scoring system used. Additionally, the Kaiser HVA tool has four matrices, which address natural hazards, technological hazards, human hazards, and hazardous materials. Terrorism is addressed throughout the different matrixes. This self-assessment tool automatically computes a threat percentage and summary of the greatest threats. Any of these tools fulfill the requirement by JCAHO in conducting a HVA to be "all risks ready." Most importantly, this should be the first step in conducting any emergency management program to prepare for threats or hazards specific to each healthcare facility.

HAZARD AND VULNERABILITY ASSESSMENT TOOL NATURALLY OCCURRING EVENTS



EVENT	PROBABILITY	SEVERITY = (MAGNITUDE - MITIGATION)						RISK
		HUMAN IMPACT	PROPERTY IMPACT	BUSINESS IMPACT	PREPARED-NESS	INTERNAL RESPONSE	EXTERNAL RESPONSE	
	<i>Likelihood this will occur</i>	<i>Possibility of death or injury</i>	<i>Physical losses and damages</i>	<i>Interruption of services</i>	<i>Preplanning</i>	<i>Time, effectiveness, resources</i>	<i>Community/ Mutual Aid staff and supplies</i>	<i>Relative threat*</i>
SCORE	0 = N/A 1 = Low 2 = Moderate 3 = High	0 = N/A 1 = Low 2 = Moderate 3 = High	0 = N/A 1 = Low 2 = Moderate 3 = High	0 = N/A 1 = Low 2 = Moderate 3 = High	0 = N/A 1 = High 2 = Moderate 3 = Low or none	0 = N/A 1 = High 2 = Moderate 3 = Low or none	0 = N/A 1 = High 2 = Moderate 3 = Low or none	0 - 100%
Hurricane								100%
Tornado								0%
Severe Thunderstorm								0%
Snow Fall								0%
Blizzard								0%
Ice Storm								0%
Earthquake								0%
Tidal Wave								0%
Temperature Extremes								0%
Drought								0%
Flood, External								0%
Wild Fire								0%
Landslide								0%
Dam Inundation								0%
Volcano								0%
Epidemic								0%
AVERAGE SCORE	0	0	0	0	0	0	0	0%

Figure 6. Kaiser Permanente HVA tool

Unfortunately, many facilities perform these analyses and address these questions because they are required to do so, not because they want to do so. This fact may hamper the usefulness of the tool and give communities a false sense of security and preparedness from their medical centers. Joanne McGlown, an expert specializing in the medical response to emergency management remarked, “Many hospital CEO’s falsely believe there is no threat” (Klein, 2003). The harsh reality is that hospitals are now being targeted by terrorists as possible locations to exercise their horrific designs. Embracing the need for terrorism and disaster response by admitting the likelihood that these events can and do occur should indeed cause facilities to be

better prepared to respond to any hazard they are confronted with. It may be appropriate to look at hurricanes Rita and Katrina and the subsequent difficulties facilities had when responding to these disasters. Senator Diane Feinstein (2005) of California commented, "Downtown New Orleans' Charity Hospital went unevacuated for days with no food, clean water, or basic medical supplies" (p. 2). NBC news reported that 40 died at the flooded Memorial Medical Center in New Orleans because evacuation efforts took too long and 34 drowned in the St. Rita's nursing home when the decision to guard in place versus evacuate was made (2005). Drawing from the lessons learned with this past year's failed disaster response to the hurricanes exemplifies the need for healthcare facilities to prepare and practice all phases of emergency management.

Security Assessment

Amid all of the effort to make sure an organization is JCAHO compliant by performing a vulnerability analysis, it is also important to review the security management plan. It is imperative that a security assessment or audit is completed in conjunction with the HVA. Suzanne Noble (2002) defines a security audit as, "a process of interviews and analyses of existing conditions, identification of potential risks, analysis of the cost of those risks to the organization, and finally, the creation of a plan to eliminate or minimize these issues" (p. 8). The security audit process compliments the HVA by treating security as a vulnerability. Consequently, the findings are then used to mitigate any shortcomings. This is often one of the last things considered, as security is a non-revenue producing entity, thus, managers have a difficult job convincing a board to fund it (Long & Pry, 2002). For this reason a security assessment checklist was developed (See Appendix B) so that facilities could perform this much needed function themselves, without needing to hire a consultant. The hospital may save thousands of dollars by performing the security audit themselves. Ideally, the security manager

should conduct the audit. However, they may not be as willing to criticize the shortcomings that exist. Paul Sarnese (1997) recommends a multidisciplinary team approach consisting of healthcare providers, nurses, facilities, and security personnel (p. 23). When a multidisciplinary team is utilized, they must be trained in standards set by JCAHO and OSHA to provide a complete and accurate assessment. Management must weigh the cost and benefit of either hiring a consultant or conducting the security audit themselves.

Security guards.

When conducting a security assessment several areas should be considered. The first component to evaluate is the security guards themselves. If the facility does not have guards, the hospital should conduct a business case analysis to determine the cost and benefit of employing security personnel. Areas to consider when performing a business case are acts of violence within the hospital, crime in the parking area, and geographic location.

Evaluation of the security guards begins by ensuring the healthcare facility is hiring trustworthy and competent security guards. Whether they are contractors or hospital staff, several things must occur. It is imperative that before a guard begins employment with any facility a criminal background check be conducted and the person is adequately trained. The key for a successful security program is the education of all staff, especially the guards. The following recommended security guard training list was developed from numerous sources of current literature:

- Patient restraint and takedown procedures
- Visitor restraint until local law enforcement arrives
- Handcuff application
- Search and seizure of weapons and contraband

- Basic Cardiac Lifesaving Skills (BCLS) certified
- Lock down procedures for the hospital
- Protocol addressing handling of media and VIP's
- Customer Service Skills
- Key strategies to prevent or respond to workplace violence
- De-escalation techniques

It should be readily apparent as to why these things are essential for security staff and how these could benefit everyone in the facility. Education is the least expensive measure you can undertake within your security management program and can prove priceless when a staff member recognizes suspicious activities and thwarts a rape, robbery, or potential terrorist act.

Security services need to be provided anytime the facility is open. If there is an emergency department (ED) or in-patient capability the presence needs to be 24 hours a day (Hodgson, 2003). The board of directors and CEO are responsible for determining what type of security presence the facility needs. However, at a minimum the ED should have security or a local law enforcement officer during the busiest times. The JCAHO environment of care standards requires hospitals to ensure patient safety and thus security staffing should be adequate to control access in the facility and safety of patients and personnel outside the hospital (Sarnese, 1997). Another suggestion is to have security guards rove within the hospital, parking areas, and perform perimeter checks to allow employees to get to know the guards and vice versa, which eases tension in critical situations because of their familiarity with one another (Klaas, 2005). Another benefit of roving guards is that it decreases the number of security guards needed to secure the area and decrease cost.

Security during emergency management.

When emergencies occur, security staff needs to have access to recall rosters, phone lists, information technology support, blue prints, emergency management plans, and evacuation routes of the hospital. This will facilitate a fast and proper response to the situation at hand. An emergency security-staffing plan must be created to ensure proper protocols for staff recall and leave cancellations in desperate situations. Several key issues determine the success of security during emergencies.

The first issue is to make sure security personnel are trained to respond in emergency management situations. Marianne Klaas R.N. (2005), states, “The security department is expected to be in the throes of any mass casualty influx resulting from a biological, radiological or chemical incident” (p. 23). Weapons of mass destruction courses and training in current threats such as avian flu should be mandatory for all security forces so they can assess potential acts of terrorism on campus grounds. To ensure the security guards safety, personal protective equipment (PPE) needs to be readily available and personnel should receive proper training on how to use it. The most important emergency management training for security forces is crowd control. As soon as patients arrive at the hospital they should be greeted at the entrance of the parking area by security and a triage nurse directing patients where to go. This will reduce the chance of possible chemical or biological contamination to the hospital. Security personnel need to be present if decontamination activities are underway to eliminate unauthorized persons on the site and control the patients being decontaminated (Sullivan & Donnelly, 2005).

Additionally, guards should be trained in the Hospital Emergency Incident Command System (HEICS) and be familiar with their roles identified on the job action sheet for security. The HEICS system is based on the Emergency Incident Command System and offers suggested

leadership positions and simple check sheets containing responsibilities for each of these positions. This system can be modified to a hospital's specific needs, but already addresses the "all hazards" response criteria.

The second key issue is communication. Generally, the largest criticism of disaster drills or actual emergency operations is the inadequacy of communication between agencies and within individual organizations. For this reason Jeff Rubin (2004) states, "This should come as little surprise because similar complaints are expressed about everyday operations – that is, a system that doesn't work well under normal conditions shouldn't be expected to do so under extreme stress" (Communications section, para.1). The HEICS system recommends that communication be centralized in the emergency operations center (EOC). The EOC acts as the brain, receiving information from all subordinate sections and then processes the data in the form of a plan. The EOC then gives the sections individual responsibilities, which allows for a collaborative response to the emergency. The transfer of information to and from the EOC will determine the success of the response. Thus, without a sufficient number of dependable communication devices, individuals may not have the best information to make decisions. Two-way radios will be of short supply as cell and regular phones may become inoperable with heavy traffic or damaged infrastructure. Whatever communication devices or system that is used needs to be dependable and running 24 hours a day so when an emergency occurs the facility is ready. The success of the security response will depend upon the communication between the guards and the EOC.

The security response during emergency management operations is vital for a successful response from healthcare facilities. However, the key security elements of communication and training are severely degraded if they are not tested regularly. JCAHO requires a minimum of

one emergency response exercise annually. Security staff must be involved in these exercises. If possible, practical exercises should be conducted semi-annually, which with the addition of more frequent tabletop exercises will ensure the proper preparation for all hazards (Rubin, 2004).

Management and staff security responsibilities.

The entire security of the hospital or healthcare facility depends upon the administration's ability to create a security management plan, ensure its implementation, and periodically evaluate compliance. It is the responsibility of the board of directors and CEO to ensure the safety of everyone within the hospital. Thus, management should make sure the following plans, policies, and procedures exist and are current:

- Emergency Management Plan (EMP)
- Security management plan
- Catastrophic emergency evacuation plan
- Workplace violence policy
- Visitor access policy
- Facility lockdown procedures
- Plan when to limit hospital access points

A separate plan for all of these items is unnecessary as long as each item is addressed within the EMP. One point that does need to be emphasized is that the catastrophic emergency evacuation plan should outline how the facility plans to remove patients out of the facility (Luizzo & Scaglione, 2004). The days of simply stating, the plan is to "defend in place" are over as seen by the horrific events that transpired because of hurricane Katrina. Too many lives were lost with the decision to stay put. Therefore, look for future legislation to enforce practicing at least partial evacuations on a regular basis.

Management also has the responsibility to coordinate with local and state agencies to ensure a collaborative response to terrorist or natural disasters. The Department of Homeland Security's report, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (2003) describes the need for health agencies to coordinate with local first responders and set in place redundant communication systems encouraging a collaborative response to disasters within the community. Healthcare administrators must be proactive in these efforts to facilitate discussion within the community to designate the hospital as a key asset and raise support for its protection during a crisis. This can be achieved by memorandum of agreements with local law enforcement. The agreement should designate a security force that will respond to the hospital during any mass casualty event supplementing the hospital's internal security (McAdams, Russell, & Walukewicz, 2004).

Hospital management is also responsible for other important aspects of security. These aspects include ensuring compliance with JCAHO security standards, annually conducting a HVA and security assessment, and regularly reviewing security issues to ensure identification and resolution of shortcomings. Another important aspect of security that management controls is the handling of terminations. This is important because disgruntled employees can be a potential cause of workplace violence. Several ways to reduce risk is by only terminating employees when a member of human resources is present, at which time access to email, patient information, and voice mail are severed. Additionally, the human resources officer confiscates keys and hospital identification badges at the time of termination. This reduces any chance the terminated employee could access restricted areas of the facility undetected to perpetrate an act of violence.

Just as management has the responsibility to provide safeguards such as policies, procedures, and physical security, the staff is responsible for applying the training they receive and maintaining their awareness within the environment. Management can help the staff achieve this goal by including security in the job description of every employee, thereby empowering them to make a difference. The following list of training was compiled utilizing recommendations from numerous sources of current literature. Thus, hospital staff's initial orientation and annual training should include:

- Workplace violence education and response
- Security awareness and responsibilities for staff
- Emergency response plan including individual staff responsibilities
- Patient decontamination and application of PPE
- Information about security codes and policies
- Procedures for accessing and utilizing emergency telephone numbers (fire, police, HAZMAT, etc.)
- Protocols to report suspicious activities

To emphasize the importance of this training, the CEO or Chief Administrator should discuss the topic of security and make it a top priority in order to help gain staff buy-in. One of the greatest benefits of getting staff buy-in is that it is inexpensive and can make a huge difference in reducing crime within the hospital (Moss, 2002). Consequently, training is of little use if the staff does not have an opportunity to practice the skills they learn. Hence, staff members should have the opportunity to participate in emergency and disaster drills at least annually.

Emergency department security.

The emergency department is the gateway to the hospital and thus should have adequate security measures in place to control access to the rest of the hospital, while protecting the patients, visitors, and staff within the department. Security measures should be evident prior to entering the ED. Vehicle access to the ED should be limited to emergency vehicles only, thus implementing a standoff distance of at least 50 meters to decrease blast effects from a car bomb. Additionally, the ED doors should have a blast film applied to windows to decrease flying shards of glass and the ambulance bay doors should be blast resistant and equipped with a keypad lock (Hodgson, 2003). Upon entering the ED, the patient should pass through a metal detector, or at the very least should see a security guard to check identification and issue a patient or visitor badge. Studies have shown that patients and staff feel safer when a metal detector is used (Simon, Khan, & Delgado, 2003). Closed circuit television (CCTV) should also be implemented and monitored as long as the facility is open. The cameras should be in view and focused on the entrance, waiting room, and ambulance bay to stand as a deterrent for violence.

Emergency department staff and security should be trained in detection of and confiscation of weapons, de-escalation techniques, and forensic evidence collection. Another precaution is to call for additional security to be present in the ED when a patient arrives with a gunshot or penetrating wound. This is especially important in areas with a high gang activity, because the rival gang member may arrive at the ED to finish the job (McAdams, Russell, & Walukewicz, 2004). Furthermore, by providing the ED with separate vending machines, restrooms, and waiting areas, the facility reduces the occurrence of unauthorized visitors roaming the halls after hours (Noble, 2002).

Security for information technology.

Information technology security begins with the creation of a disaster recovery plan (DRP). “A DRP is a comprehensive program detailing how an organization will react to destruction of or severe damage to vital computer information. In addition to natural disasters it should also address: power outages, worms, virus attacks, and hackers” (Grigsby, n.d.) Disaster recovery plans are required by the health insurance portability and accountability act (HIPAA). The main thing to take away from the DRP is the answer to how the facility will backup data and whether the backup should be located on or off-site. Moreover, the data information center must be located in a restricted access area and be secured by locks, keypad and video surveillance (Hodgson, 2003). This is especially important if your facility is utilizing the electronic medical record.

Other elements of security for information technology exist as software and hardware on the network. Hardware security measures consist of firewalls, routers, switches, and computers. Software and protocol measures include passwords, firewalls, antivirus, security patches, browser controls, VPN, SSL, and encryption. These security measures coupled with monitoring the network for unauthorized access will help to ensure data integrity. As healthcare increasingly becomes more automated and information driven, the information technology departments of hospitals will continue to grow in numbers of employees and budgetary requirements. This will require agencies to spend more on securing important healthcare data.

Facility security measures.

Utilities are the lifeblood of the hospital, because if there were no water, power, or gas, the facility would cease to function. It is for this reason that special attention needs to be taken with the security of utilities. Thus, the hospital’s power plant including water, generator, and

telephone, needs to be secured by fencing, locks and monitored by CCTV 24 hours a day (Klein, 2003). Additionally, healthcare facilities should not feel overconfident that arson is not a threat just because there is a sprinkler system. Each sprinkler system has a secure open stem and yoke (OS&Y) valve, which controls the sprinklers. If this valve is not protected, then an arsonist could shut the valve and set a fire. The OS&Y valve is supposed to be chain locked, but it could also benefit from a fence and CCTV coverage. The facility is required by JCAHO and Occupational Safety and Health Administration (OSHA) to check all fire equipment on a monthly basis to make sure everything is functioning properly (Arterburn, 2002).

Another item of great importance is the protection and security of air intakes and Heating Ventilating and Air Conditioning (HVAC) system. If these are located on the ground, it is easy to contaminate the air supply with chemical or biological agents. The HVAC system could then be used as a dispersion device for the agent. It is necessary that hospitals consider relocating any intakes that are at or below ground level to at least 12 feet off the ground so it will be out of reach of someone on the ground. However, the higher the intakes can be placed the better (Department of Health and Human Services, 2002). Furthermore, parking areas are often vulnerable to crime. Adequate lighting to overlap areas from one pole to another must be achieved to eliminate shadows when a light is out. Facilities should also consider placing cameras in the parking areas to decrease the chance of rape or theft (Hodgson, 2003).

The hospital needs to ensure compliance with OSHA and hazardous material (HAZMAT) standards for sensitive items storage. Arterburn (2002) and Luizzo & Scaglione (2004) suggested the following:

- Biohazard materials placed in locked freezers, incubators, and cabinets
- Inspect HAZMAT data sheets and secure hazardous chemicals or agents

- Radioactive materials are in a restricted area and secured from visitor access
- Oxygen tanks and other medical gases storage area is physically secured by fencing, locks and monitored via CCTV
- Gas and oil tanks are physically secured by fencing, locks and monitored via CCTV

Storage is a big concern when the items could be used in a terrorist attack and thus any hazardous agent must be accounted for and secured (Luizzo & Scaglione, 2004). Facilities are also responsible for signage in and outside of the hospital. Outside of the facility, signs need to direct patients in order to prevent them from wandering into unauthorized areas. Inside the facility, signs should clearly mark off-limits areas with “Authorized Personnel Only” and direct patients to high traffic areas. Adequate signage will help to increase patient satisfaction because they will not have to ask staff where to go as much and it will help to ensure patients are where they should be (Hodgson, 2003).

Securing hospital access.

Within the security assessment, securing hospital access is the most difficult to functionally achieve because there has to be a balance between accessibility and security. The facility must remain inviting and calming for patients and visitors yet ensure that sensitive items are beyond the grasp of those who would seek to do harm (Healthy Options, 2002). Hospitals located in a high threat area, such as urban city centers or national points of interest, should consider a vehicle checkpoint placed away from the hospital. The following are procedures for operating a vehicle checkpoint and were compiled from suggestions found in multiple sources of literature:

- Incoming deliveries are screened to ensure no explosives or dangerous materials are entering the campus, then allowed to proceed to the loading dock
- All vehicles screened with a minimum of the driver showing an ID and reason for visit, then the driver given a vehicle pass.
- Facility has installed vehicle barriers as needed according to HVA
- After hours deliveries procedures are in place
- Monitored by CCTV

It is important that security be able to differentiate employee vehicles from those of patients and visitors so that any suspicious vehicle may be identified. This includes hospital – owned autos such as ambulances or other emergency vehicles (Arterburn, 2002). Along with screening vehicles, all persons entering the facility must be screened utilizing the appropriate level of precautions determined by the HVA. The following recommended procedures for high threat areas were developed from numerous sources of current literature:

- Employees wear their badges at all times while on campus
- Employees name is large enough on badge to be read easily and has a color photo stating what department they work in, credentials they hold, and an expiration date
- Procedures exist to handle lost / stolen ID cards and what employees must do when they arrive without one
- Visitors will show ID and sign-in and out and receive a visitor or patient badge which must be visible at all times
- Bags and boxes screened for weapons and contraband

- Policy in place for refusal of access to people who do not have positive identification or do not have a legitimate need to enter the site
- All contractors / vendors report to a central site to sign-in and receive distinct badges
- All visitors, patients, contractors, and vendors briefed about authorized areas they can go within the facility
- Policy that if visitors are found without a badge they will be escorted to security

Additionally, it is also better if the facility utilizes one main entrance to funnel the traffic where the hospital wants the visitors and patients to be. This helps to deter crime because the perpetrator would have to exit where they are being monitored (Hodgson, 2003).

A less invasive approach to monitor high-risk areas is the use of CCTV. Cameras can be placed almost anywhere and have the ability to be viewed and recorded via the computer network. This is a nice tool for administrators and security staff to be able to see what is going on in the facility from any computer (Leonidas & O'Donnell, 2005). Initially, there is a high cost to install CCTV. However, savings can be realized by reducing security staffing. One of the benefits of CCTV is that it takes fewer security guards to monitor the campus. Several other areas that should have limited access are the pharmacy, laboratory, medical records, and the mother – baby unit. These areas should have keypads or locks installed, CCTV monitored during operating hours, and roving security. It is important to realize that access to care does not mean access to the entire facility. The world has changed since 9/11 and the healthcare industry must adapt to the new threats. Hospitals that embrace security will be better prepared to deter terrorism and crime on campus.

*Hazard Management**Terrorism and crime mitigation.*

Unfortunately, assessing the local threats to a facility is not enough. Once the hazard vulnerability analysis is complete, the identified threats can be mitigated through controls. Jerry Mothershead (2004) describes mitigation activities as controls taken to eliminate or reduce the vulnerability of the facility to threats through deterrence and prevention. Furthermore, Fredrick G. Roll, President of Roll Enterprises explains how to mitigate terrorism by asking, "If I wanted to shut this place down, what would I do and how? Then put counter-measures in place to prevent that from occurring" (Hodgsen, 2003, p. 18). Asking this question is the key to protecting hospitals. One must first think about possible strategies that a terrorist might use to target a facility, before creating a plan to defend against it. Administrators' hoping that their facility will not be subject to terrorism is certainly a strategy some might employ. However, initiating a plan to mitigate weaknesses within a hospital will not only help protect it from terrorism, but also from violent crime on campus.

A realistic approach to protecting your staff, patients, and visitors must be a coordinated effort in response to real threats facing the hospital. Terrorism may be a distant threat in rural areas compared to urban city centers, but it still needs to be addressed. A more practical approach for clinics and rural facilities is to secure themselves against violent crimes. "According to the National Institute of Occupational Safety and Health, hospital workers experienced assaults at the rate of 8.3 per 10,000 employees in 1999, more than quadruple the two assaults per 10,000 employees in other sectors" (Shinkman, 2003, p. 10). Many of the mitigation techniques, which protect patients, employees, and visitors, may be effective in deterring terrorism as well. Administrators should not hesitate to employ terrorism mitigation

techniques because many of them do not carry a high price tag. The cost associated with terrorism prevention is certainly a factor when choosing which techniques to use. For this reason, I created a matrix to provide administrators with options for implementing terrorism and crime prevention techniques within their facilities (See Appendix C). The terrorism mitigation matrix also provides products and vendors with a per unit price for each product included. These vendors and products were chosen randomly using internet search engines and no endorsement or payment was received to advertise these vendors or products. They are meant to be a resource to save time and provide information about current technology and existing programs.

Terrorism mitigation techniques can be divided into several categories: procedural, training, technology, and architectural design. Each of these categories provides different approaches to prevent terrorist attacks. Some of these techniques are very inexpensive and some should be reserved for urban areas that are more prone to terrorist and crime activity. Each facility differs in needs, financial stability, regulatory requirements, and restrictions, which make it impossible to create a specific list of products or measures for each hospital. Therefore, the following is a general discussion of areas hospitals must address in order to determine if threats facing each facility require a mitigating technique to reduce the risk.

Procedural techniques.

Simply adjusting inadequate policies and procedures will strengthen security measures at any facility. Of course, the price is right too. Generally, there is little to no added cost from exercising procedural techniques designed to combat terrorism. Some procedural policies or techniques that can strengthen security measures are:

- Visitor access control policy exists and is up to date
- Employment of security forces

- Security management plan exists and is up to date
- Emergency response plan exists and is up to date
- Loading dock / receiving protocols exists and is up to date
- Mailroom safety protocol exists and is up to date
- Stockpiling of immunizations / antibiotics / antivirals for community response
- Procedures in place to access the Strategic National Stockpile (SNS)
- Employee ID badge policy exists and is up to date
- Community collaborative partnerships exist
- Advocate for workplace violence legislation

This list was developed from suggestions found in numerous articles in the current literature.

These policies and procedures should be evaluated annually to ensure they still meet the needs of the health center. In the security assessment section, techniques were discussed to assess a hospital's security program. In this section, the discussion of the same techniques will focus on available products, best practices, and services available to healthcare facilities to strengthen the hospital's security program.

The most important procedural technique for a facility is to ensure that the following plans and procedures exist and are up to date; security management plan, emergency response plan, loading dock and receiving protocol, and mailroom safety protocol. The security management plan will outline exactly how the facility plans to conduct security by determining responsibilities for the who, what, when, where, and why. It should also state how often to review the plan. The components of the plan should contain a threat assessment, vulnerability analysis, security assessment, and terrorism mitigation techniques, which should be incorporated into the hospital's strategic plan and made adjustable to the hospital's needs. Either the hospital

board or a consultant can assist in accomplishing these tasks. The emergency response plan should outline simple plans and procedures during emergency operations for the staff to follow, ensuring the safety of employees, visitors, and patients. As previously discussed, the HEICS system can be used as a model to develop the health center's emergency response plan. The national standard for hospitals emergency management program is the HEICS system, which can be downloaded free of charge at <http://www.emsa.ca.gov/Dms2/download.htm>.

The loading dock and receiving protocol should address how trucks are authorized to visit the dock, vehicle and supply inspection, and driver validation. The policy must also address the need to immediately process and inspect shipments prior to moving them inside the facility (Arterburn, 2002). Many sample procedures are available online, one of which is at http://securitysolutions.com/mag/security_security_hot_spot_3/.

Mailroom security received increased attention during the anthrax scares in 2001. The likelihood your facility will be the victim of anthrax contamination may be remote, but other dangers exist such as explosives, which require attention. The United States Postal Services (USPS) suggests procedures that will help your security, which can be found at <http://www.usps.com/communications/news/security/mailcenter.htm>.

Visitor access control is undoubtedly the most difficult task to accomplish in hospitals. This is usually because of multiple entrances and exits coupled with the volume of patients, employees, and visitors that enter the hospital on a daily basis. Nevertheless, controlling access within the facility can be made much easier by using sign – in sheets and ID badges that are distributed at the entrance. This helps the staff identify visitors from patients and allows them to direct visitors to appropriate places within the hospital. There are many products available to assist with this task. One is a carbon – backed commercial sign – in sheet that produces a

temporary badge for patients and visitors to wear and provides a record of who entered the facility. This is a relatively low cost solution to access control. In addition, many hospitals have produced their own sign-in sheets and use badge holders to carry their driver's license or other picture ID while in the facility.

This may prove to be a difficult process if the facility has a large number of entrances. Management should consider reducing those numbers, if necessary. It is best if the hospital utilizes a main entrance with a reception desk to sign-in at and personnel to direct patients where to go (Arterburn, 2002). A security guard could run the reception desk providing an initial security presence where patients and visitors enter the facility. Employing a security force is a tough decision for management, because the service is a non-revenue producing expense. However, when a violent act occurs within a hospital, managers and boards are willing to purchase very costly items or services to combat violent crime (Long & Pry, 2002).

Another procedural technique is to require staff members to wear photo ID badges listing name, credentials, department, and the expiration date of the badge (Arterburn, 2002). Even if the person plans to stay for years, a new ID needs to be created every couple of years because people's identifying characteristics change over time. How often have you observed an ID where someone looks 10 years younger, has a mustache, and a full head of hair? Now that person is bald, wears glasses, and no longer has a mustache. There are a multitude of computer programs that will create ID badges and the price range is just as variable. The ID's will print on either a regular printer or a specialized ID printer, which will print on plastic badges or other material. Smaller health centers where everybody knows each other could use a cheaper program, where the danger of creating a fake ID badge is relatively low. However, larger facilities should consider using a program that allows holograms and other high-tech options to deter counterfeits.

Membership within community collaboratives or community-based organizations provides excellent opportunities for hospitals to help strengthen their emergency response capability. These organizations help to combine resources within the community that can be mobilized during an emergency and help augment the healthcare response. Memorandums of agreement or understanding should be written to outline exactly what each organization will do before, during, and after an emergency. These groups also may be able to assist the local health organizations to lobby for legislation to fight workplace violence within hospitals by asking laws to be passed making assaults occurring against healthcare personnel felonies. Some states have been successful in implementing such laws and have seen a decrease in healthcare related violence.

Of current and future concern is the ability of healthcare organizations to respond to local, national, and worldwide epidemics by maintaining a local immunization and medication stockpile. Whether the threat is natural such as the avian flu or manmade biological terrorism, emergency departments and public health agencies need to be ready to treat affected patients. Nevada Hospital Association created a model and plan to deal with these scenarios, which can be downloaded at <http://www.nvha.net/bio/postings/prophyguide.pdf>. This plan also discusses the need to ensure the safety of the family members of hospital workers and suggests procedures by which this may be accomplished. By taking care of the family members, there is an increased chance that healthcare workers will show up for work during biological emergencies (Bullard, Strack, & Scharoun, 2002).

It is also necessary for communities to understand how the Strategic National Stockpile (SNS) is accessed and the political chain that needs to be contacted to grant federal aid. The state governor has to contact DHS or the CDC to request SNS support. Discussion of the process is

found on the CDC website at <http://www.bt.cdc.gov/stockpile/>. These procedural techniques to combat terrorism can be very inexpensive if the facility chooses to provide current manpower to accomplish the tasks involved. High-risk hospitals should consider hiring a security consultant to ensure appropriate mitigation of threats through the development of plans and procedures.

Education and training.

Education and training is another terrorism mitigation technique effective in decreasing a hospital's risk from attack. The risk decreases because employees increase their awareness about terrorism, as well as their environment. A myriad of training programs exist to educate employees about terrorism ranging from no cost to high cost. I suggest the following topics of training for hospital employees:

- Basic Terrorism Awareness
- Gang Awareness
- Chemical, Biological, Radiological, Nuclear, Explosive (CBRNE) Training
- Security Competency Training for Security Staff
- Diagnosing Chemical and Biological Illnesses for First Responders

Training hospital employees does not have to be time consuming and cost prohibitive as there are many free online training sources for antiterrorism. This training should encompass an overview of terrorism including what to look for and how to spot suspected terrorist acts. A free basic interactive tutorial about terrorism can be found at <https://atlevel1.dtic.mil/at/>. Another useful website lists free training that the federal government sponsors. It is located at http://www.fema.gov/compendium/course_search.jsp?style=FEDDEPARTMENT.

Advanced training about terrorist weapons or CBRNE training should be mandated for all triage personnel and physicians, because these providers will be responsible for their care if they

arrive at your facility. The triage nurse has the greatest responsibility for ensuring the emergency department does not get contaminated by one of these patients and should be familiar with the signs and symptoms of CBRNE attacks (Sullivan, & Donnelly, 2005). This great responsibility on the emergency department will be reduced, if the staff feels comfortable and knowledgeable about CBRNE injuries. A complimentary online course is provided for healthcare personnel at <http://www.swankhealth.com/USAMRIID.html>. It is imperative that hospital staff receive training because, "Emergency departments will not only respond first, but will deal with a multitude of issues surrounding a bioterrorist attack...These split-second decisions will often draw the line between who lives and dies" (Sharoun, Caulil, & Liberman, 2002).

Gang awareness training is suggested for all health centers and should be mandated for inter-city hospital employees. The National Alliance of Gang Investigators Associations (2005) remarked,

Once found principally in large cities, violent street gangs now affect public safety, community image, and quality of life in communities of all sizes in urban, suburban, and rural areas. No region of the United States is untouched by gangs. Gangs affect society at all levels, causing heightened fears for safety, violence, and economic costs (p. 6).

Hospitals should contact local law enforcement agencies to schedule in-service training about community gangs, their culture, and information of how to recognize and react to potential violence.

Finally, security forces competency training should be required for all hospital security personnel. This should be written into the contract, if the guards are contracted through a larger corporation. Personnel need to ensure that the guards are qualified and have the necessary training for the hospital environment (Gonzalez, 2002). Marianne Klaas R.N. states that

knowledge of HEICS, meet and greet, environment of care and safety, restraints, crisis and workplace violence prevention, handcuffs and forensics, weapons / drugs surveillance and confiscation, as well as, local and state criminal codes and standards, should be required of healthcare security officers (pp. 22-23). There are several agencies that certify security professionals, which may help to ensure a hospital's security services are adequate. The International Association for Healthcare Security and Safety (IAHSS) provides a certification specifically for hospital guards. They provide training materials and offer basic and advanced certifications via onsite and self-study courses in healthcare security requiring the participant to pass knowledge based exams prior to earning the certification. Information about obtaining IAHSS certifications are found at http://iahss.org/cert_welcome.asp.

Technology mitigation measures.

Technology can assist greatly in mitigating terrorist threats. This section will provide brief descriptions of current technologies that may assist hospitals' security efforts. Specific pricing and sources for these products are found in the Terrorist Mitigation Matrix (Appendix C).

Metal detectors are quickly becoming commonplace at large venues, government buildings, and the emergency department entrance. Placing a metal detector in the emergency department often makes patients and employees feel safer (Simon et. al, 2003). Subsequently, metal detectors coupled with continued awareness and training of staff can help to deter violence and terrorism in the emergency department.

Several technologies exist to help prevent unauthorized access to sensitive areas within facilities including keypads, keycards, proximity cards, manual locksets, biotechnology recognition, intrusion alarms, and passive door alarms. Since 9/11, the Office of Homeland

Security is urging hospitals to screen all incoming persons, upgrading to card access technologies, dead bolts, door alarms, and utilization of CCTV (Luizzo & Scaglione, 2004). All of these systems accomplish the same thing, which is to stop unauthorized access.

For this reason, it is only necessary to define or describe what each device does. Keypads are generally a numbered 9 – 10 digit pad located outside of sensitive areas requiring access codes for entry. Keycards generally have a magnetic strip that must be swiped in a card reader located outside doors to a sensitive area. Proximity cards are similar to keycards except the card only has to come within a certain distance to the sensor causing the door to open. Manual locksets are tried and true security, but remain inconvenient for high volume access. Biotechnology such as iris or fingerprints scans are resistant to theft and counterfeit, assuring access to only authorized personnel. Many theme parks are utilizing this technology for season pass holders to reduce the loaning of passes to others and the loss of revenue. Intrusion alarms combine infrared sensors, passive microwave, and perimeter-sensing capabilities to ensure unauthorized access cannot be achieved at the perimeter of the grounds and sensitive areas within the facility. Passive door alarms are simply magnetic contacts alerting personnel, when an emergency exit door is opened. The difference between these technologies is the level of convenience the system can offer including multiple functions that may even reduce the need for a larger security staff. For instance, if the emergency department is isolated by an access system, the chance of unauthorized, after-hours access to the rest of the hospital greatly diminishes.

Communications are generally a headache for hospitals even when everything is running smoothly. When emergencies occur, communication may break down. The number one concern that arises after disaster drills is the need for better communication equipment and more of it. Building redundancy into the communications system is imperative and can be accomplished

with satellite phones, emergency-banded communication systems, and pa systems (Glick, Jerome-D'Emilia, Nolan, & Burke, 2004). The main requirement for a communications system is the ability to stay in contact with other hospitals, law enforcement agencies, and public health channels. As long as the system can accomplish this and provide enough units for internal communication, it should be adequate. One option is a starter communication system found at http://www.warningsystems.com/starter_system.htm.

Explosive and chemical detection devices are technologies available for vehicle and cargo inspection stations. These are hand held devices offering maximum portability and flexibility for defense against terrorism. This is extremely important, because one of the most likely terrorist threats is a vehicle borne improvised explosive device (IED). One option for detection devices is found at http://www.sitebuys.com/explosive_detector.html.

Infant abduction systems have become very sophisticated with RFID technology. A bracelet or ankle band is placed on the baby and then monitors are placed throughout the facility to determine the exact location of the infant. This is usually accompanied by an alarm that is triggered if the baby is removed from the mother baby unit. This technology also may be attached to equipment, decreasing theft of wheelchairs and other easily lost items (Noble, 2002). One example of the product can be found at <http://www.securecare.com/KinderGuardID.htm>.

Disaster recovery plans for information technology systems are quickly increasing in popularity and necessity. JCAHO requires a disaster recovery plan for information systems to be in place to mitigate disasters (Joint Commission Resources, 2005). As the medical record becomes electronic and hackers and other criminals attempt to acquire and or destroy this information, redundancy of data is necessary. These plans call for secondary data repositories to be housed at a separate location from the primary site. New contractors are offering these

services at an affordable rate to ensure data is not lost (Grigsby, n.d.). One such disaster recovery service is found at <http://www.agilityrecovery.com/>.

Panic buttons are old technology being utilized in new ways. Many facilities are placing panic buttons where money transaction takes place or at reception desks to notify security of problems. This is a very simple low cost option to help decrease violence (Klein, 2003).

CCTV is becoming more useful with new technology. Options such as digital recording, facial recognition software, thermal cameras, day / night cameras, and motion – sensing cameras offer significant upgrades and are possibly the greatest security tool for hospitals (healthy options, 2002). Digital recording allows continual recording during playback modes, as well as, affords the opportunity to view camera feeds from any computer on the network. Facial recognition software stores video clips of individuals within the facility. It also offers the ability to go back into video logs and pull all possible encounters with a person that have been in the facility as long as a security camera recorded them. This technology helps to identify perpetrators of theft, recently fired personnel, and anyone who has caused problems on campus in the past.

New cameras such as the thermal camera allow security staff to locate intruders in the dark or hiding behind objects by illuminating heat signatures. Another useful camera is the day / night camera, which offers high-resolution color feed during the day and monochrome feed during the night. Additionally, motion sensing cameras focus on movement around them and then go back to a standard position when no motion is detected (Leonidas & O'Donnell, 2005). These new technologies can certainly augment current CCTV devices hospitals utilize and they offer more options to deter crime, violence, and terrorist activity. Examples of each of these technologies, including websites are contained in Appendix C.

Achieving terrorist mitigation through design.

Terrorist threat mitigation by design is ultimately the highest measure of protection a hospital can provide. This type of mitigation is necessary when all other security measures fail and a breach occurs. A hardened facility will have the best chance of protecting employees, patients, and visitors from blast effects. The best example of a hardened facility is in the heart of Washington D.C.. Project ER 1 is the best practice for mitigating terrorism through design. More information and resources utilizing design as a threat mitigation tool can be found at www.er1.org. Dr. Michael Pietrzak, the director of ER one states, “The thought process behind it is if you design from the ground up, ultimately you have more capability , and it can be done at less cost than a retrofit” (Hodgson, 2003, p. 22). This begins with an architect who not only has experience designing hospitals, but also with security engineering. Next, the board must determine what Dr. Pietrazak calls the ‘critical axis,’ which are “specific areas and infrastructure that are essential to maintain the effectiveness of the hospital” (Pietrzak, 2004, p. 1). These areas may include the emergency department, intensive care unit (ICU), surgery suites, laboratory, radiology, pharmacy, food supplies and services, and facilities such as water, med gases, power, ventilation, and communication systems (Pietrzak, 2004). Once the critical axis is determined, the architect then can implement design modifications to protect these areas against perceived threats, taken in order of likelihood from the HVA.

This section will discuss design measures to mitigate possible terrorist attacks. Each design measure is associated with an actual product to utilize as a resource found in Appendix C. However, this independent product research should not be considered as best pricing or the best product that exists. They are meant to give the reader a general idea of what each measure might

cost in a facility and they do not include the labor price to install them. These figures represent per unit costs and each design measure may require multiple units to incorporate within the overall security management plan.

One of the simplest design measures is to ensure parking areas have adequate lighting. Proper lighting will help alleviate crime such as vandalism, theft, and rape. Most hospital staffs are comprised of women and they must feel safe, especially in today's competitive nursing environment. Hospitals likely will fall subject to a nursing shortage if the facility cannot protect the staff (Long & Pry, 2002). The parking lot lighting design needs to have overlapping cones of light so that if one light burns out there still will be adequate lighting within the area (Hodgson, 2003). Lighting itself will not solve all of a facilities parking lot issues but coupled with technology and roving guards, most crime should be eliminated.

Another design measure is the location of nursing stations on wards. This can play an integral part in decreasing security manpower requirements by having employees' eyes on the entrance and exit of a ward constantly. This of course is of utmost importance on the mother baby unit to protect the innocent and helpless from abduction (Hodgson, 2003).

Decontamination site location is critical during HAZMAT and CBRNE incidents. A contaminated patient who is allowed in the facility may quarantine part or all of the hospital and cause it to become closed to normal operations. The hospital should be locked down during decontamination operations and the emergency department then becomes the point of entry once the patients have been decontaminated. The decontamination site should be located away from the main facility, as it is very difficult to keep from contaminating other areas of the hospital. Mobile DECON shelters or a separate building away from the main facility can reduce the possibility of hospital contamination (Siegelson, 2000). Not only is the location a design

consideration, but also the collection of contaminated water. The disposal of this contaminated water must comply with local and state environmental regulations including those mandated by the Environmental Protection Agency (Vogt & Sorensen, 2004). This collection may be easier if a permanent structure is built with drainage to a large collection tank.

Air handling in hospitals is a massive design issue with real consequences for protecting the facility from terrorism if safety measures are not taken. HVAC systems can be built with materials that decontaminate themselves such as ionic silver plating. Additionally, the use of HEPA filters, which remove 99.97% of particulate matter, reduces the risk of chemical and biological contamination in the hospital. Furthermore, laboratory and clinical personnel working within a biological testing environment will require negative pressure ventilation. This is a precaution because of the possibility the lab will have to operate at maximum capability during a biological event (Siegelson, 2000). Of most importance are the air intakes to the HVAC systems. These should be located at least 15 feet off the ground and have a mesh metal grate covering the inlet. This inlet should be sloped at a 45-degree angle to keep from having substances thrown into the intake (See Figure 7).

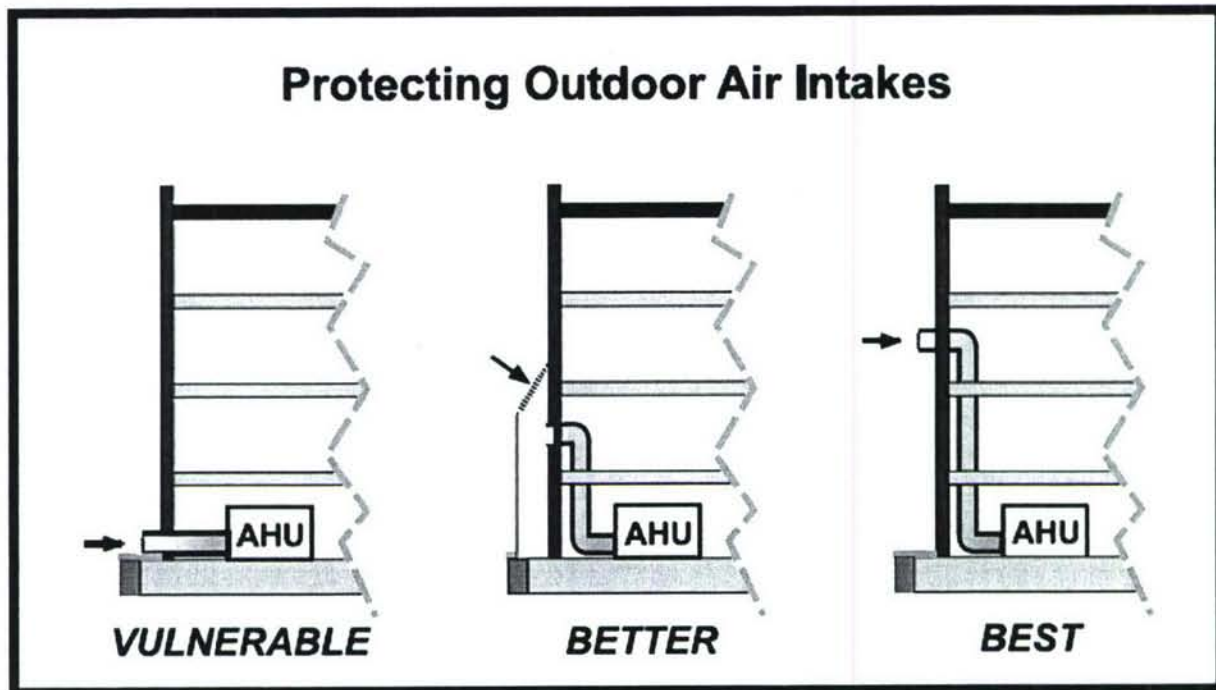


Figure 7. Protecting outdoor air intakes from (Department of Health and Human Services, 2002).

For more information about HVAC and intake systems visit www.cdc.gov/niosh/bldvent/2002-139.html.

In addition to HVAC systems, surface decontamination should be a high priority. Blister switches rather than traditional toggle switches are easily cleaned and decontaminated. The use of seamless surfaces combined with rounded corners eliminates areas that are hard to decontaminate. The use of ultraviolet light kills airborne bacteria and reduces the chance of nosocomial infections. Combining these design measures with self-decontaminating materials such as paint, treated wall coverings, and ionic silver drains, will result in a room that is highly resistant to bacteria and cross-contamination of patients (See Figure 8). Surface technologies and design measures combined with HVAC systems help achieve an immune hospital environment (Pietrzak, 2004).

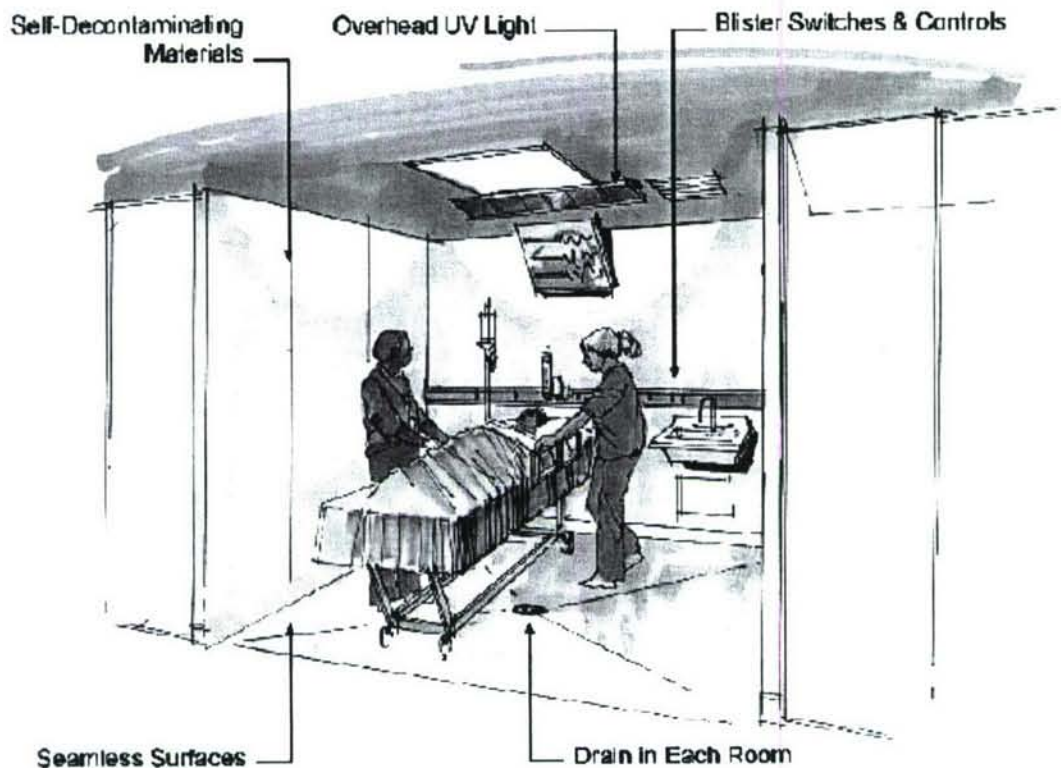


Figure 8. Surface technology for immune building environment (Pietrzak, 2004).

Design measures can help ensure only authorized access onto campus grounds. This begins with a fence, wall, or change in landscape to differentiate the hospital property from surrounding businesses or the community. These simple measures will help funnel patients, visitors, and staff to authorized vehicle and pedestrian entry points. Vehicle checkpoints screen in-coming vehicles for explosives and weapons that could harm individuals or damage the facility. The design of these checkpoints is crucial to its effectiveness. There must be bollards and pop up barriers to keep vehicles from ramming through the checkpoint. An example of a checkpoint is shown in figure 9.

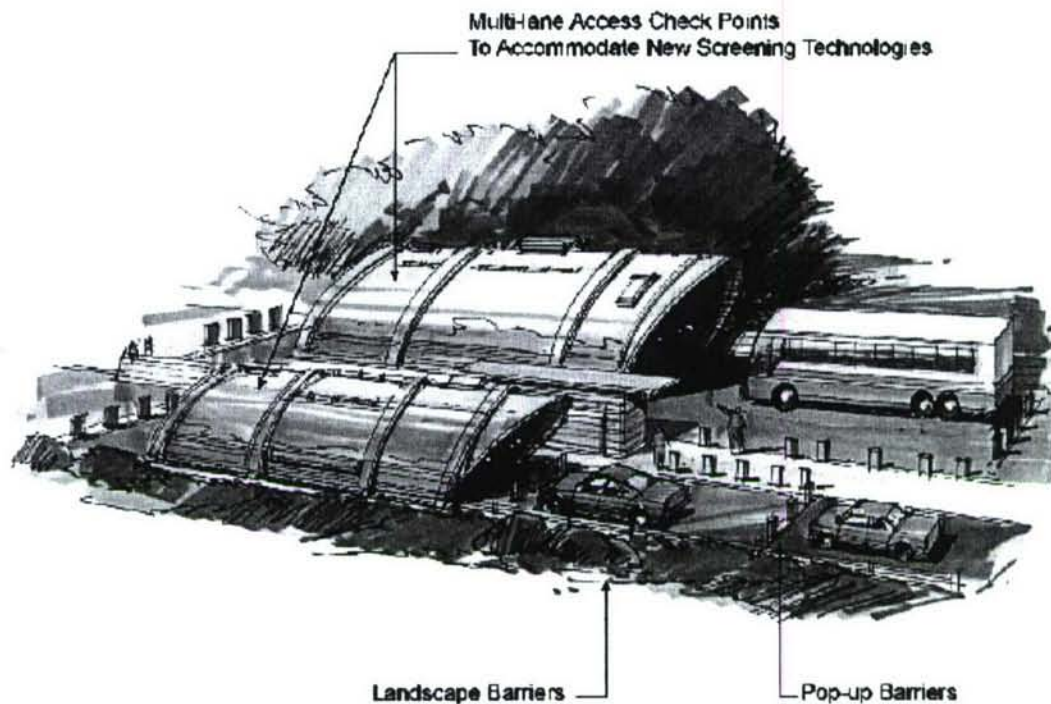


Figure 9. Vehicle checkpoint design (Pietrzak, 2004).

Design measures for blast mitigation undoubtedly offer the greatest protection for those within the facility, but are often expensive in their implementation. Administrators must review their HVA and determine what measures are necessary to protect patients and employees. The most useful design measure and cheapest in mitigating blast effect is standoff distance (Pietrzak, 2004). Standoff distance is the distance between the building and barriers or natural landscape, which a vehicle could not gain access. The main reason this is so important is the energy from the blast wave dissipates very rapidly and the greater distance from the blast, the less damage occurs. The Department of Defense (DOD) implemented new design standards as depicted in figure 10. The required minimum standoff distance from a controlled perimeter for new DOD construction is 25m or 82ft (FEMA, 2004).

DoD Stand-off Distance

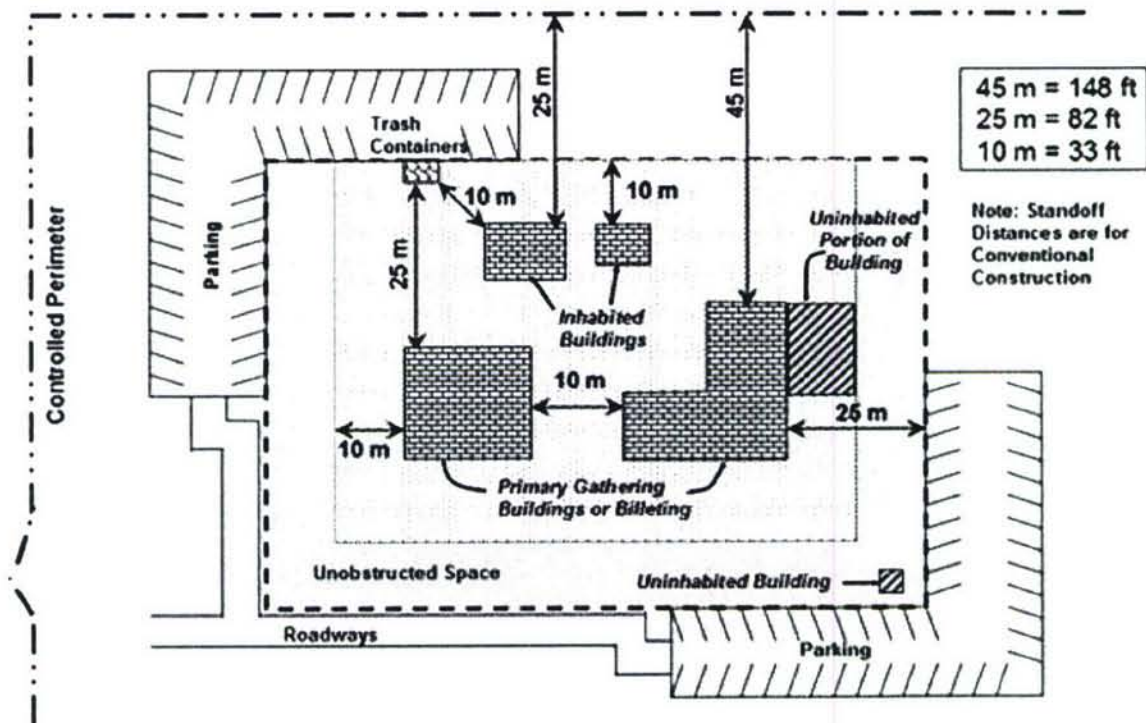


Figure 10. DOD standoff distance for new construction (FEMA, 2004).

Landscape features may be utilized like bollards for standoff distance. Larger mounds and boulders may serve as natural blast walls to decrease blast wave propagation. If landscaping is not an option, blast walls and external facade shields can provide even better protection for buildings on campus. Blast walls are generally large reinforced concrete barriers located on the perimeter of campus next to roadways. The façade shields are panels that absorb blast effects and minimize damage to the building structure. Heavy concrete is used when building new projects in order to minimize blast effects, as well as provide radiation protection. Concrete is a superb material for attenuation of radiation. Additionally, ferric particles can be added to the concrete to provide further protection against radiation (Pietrzak, 2004).

Recent concern has been expressed related to the prospect of an ambulance approaching the emergency department entrance and detonating a vehicle borne IED. This scenario could be mitigated by designing emergency departments such that they could prepare for a blast. Blast mitigation measures for buildings include doors and windows. The hospital should consider installing a blast resistant ambulance bay door in the emergency department and possibly design the ambulance bay away from a main corridor. This would eliminate a direct line of sight between the door and the department (Hodgson, 2003). Windows can have an anti-shard film applied to them, which decreases the chance projectiles are created in the event of a blast. Another alternative is to purchase blast resistant (bulletproof) glass for high-risk areas.

An overlooked mitigation measure in design is to use overpressure outlets that will decrease the blast wave pressure inside buildings, thus decreasing damage to the building and the severity of injuries to personnel. "The degree of damage resulting from the blast wave depends upon the magnitude and duration of the peak overpressure, which, in turn, depends upon the explosive force and the environment in which the explosion occurs" (Frykberg, 1988, p. 573). The overpressure outlets allow the pressure a way out of the building without destroying walls. An example that some might be able to relate to from their youth is that of a large firecracker and a mailbox. If you place that firecracker in the mailbox and just close the box door, the door will fly open and there will be little damage inside the box. However, if you take that same firecracker, place it in the mailbox, and secure the door with tape, the mailbox will likely be destroyed. The overpressure outlets work in the same way allowing the pressure to escape and decreasing damage to the rest of the structure.

Internal blast mitigation techniques include anti-shard wall coverings and compartmentalization. Anti-shard wall coverings are panels, which have KEVLAR or another

material that protects inhabitants from flying objects in the event of a blast.

Compartmentalization is a design technique used to zone off or compartmentalize components within hospitals. It may involve strategically placing hallways in between outside walls and departments or other similar buffering types of design (Hodgson, 2003). The bottom line for all of these terrorism mitigation efforts is that it is far cheaper to implement them in the initial design and building of facilities than to try to retrofit them later. Those facilities for which retrofitting is not an option, can significantly reduce the chance of damage by terrorism through updating their policies and procedures, implementing antiterrorism training programs, and utilizing new technologies for hospital security.

Preparedness Phase

Hospital emergency management is a complex multifaceted and resource intensive obligation that healthcare facilities must facilitate. There are many opinions about what should be done and how to perform emergency management functions. Emergency Management is well documented and there exists somewhat universally accepted techniques to address requirements facing hospitals. For this reason, only a short summary of techniques will be presented.

The four phases of emergency management consist of mitigation, preparedness, response, and recovery. The mitigation phase has already been discussed in the threat assessment and hazard management sections, which consists of identifying hazards and threats culminating with the development of an HVA and implementing controls to mitigate the threats. The preparedness phase includes planning, training, and conducting exercises to test, evaluate, and revise a facility's emergency management plan (Mothershead, 2004). Planning is the key that opens the door to success. The old adage, "if you fail to plan, you plan to fail," remains true today.

Disaster Planning

The result of disaster planning in hospitals should be the creation of the emergency management plan. The EMP itself is useless if it is created with the sole purpose of maintaining JCAHO accreditation or is not followed when the emergency occurs. The EMP needs to be a functional tool that is implemented easily in the event of an emergency to facilitate the medical piece of incident management within the hospital, locally within the community, and regionally in support of larger disasters. This does not mean that the first time an individual opens the EMP is during an emergency. Rather, they should be familiar with their roles and responsibilities and be trained to act in whatever position they hold. However, since we cannot choose when emergencies occur and will not be guaranteed to have all of the trained personnel available, the EMP must be simple enough that anyone can respond by fulfilling the required responsibilities. According to K. Joanne McGlown, Ph.D. (2004, p.16), a healthcare facility's plan must address the following:

- Risk analysis and hazards vulnerability analysis
- Incident Management
- Surge capacity
- Protection of direct caregivers
- Provision for continuity of the daily (standard) levels of care
- Management of mental health and special – population needs
- Public education and involvement
- Redundant communications and process capabilities
- Periodic testing through communitywide drills and exercises
- Types and quantities of PPE and other protective items to be stocked

- Decontamination capabilities
- Regulations and standards that direct or mandate action

Additionally, Donald White (2002), director of safety and security at the Northern Virginia Mental Health Institute suggests the following considerations when developing emergency response plans:

- Power
- Foodstuffs
- Utility water treatment
- Medication
- Communications
- Shelter
- Transportation
- State agencies
- Local agencies
- Personnel
- Vendors

Furthermore, JCAHO has provided a checklist for emergency management that also addresses considerations for disaster preparedness (See Figure 11).

Emergency management checklist

	Issue assessed	Action plan developed	Staff contact assigned
Identification of authorized personnel			
• Individual designated as incident commander on all shifts			
• Lines of authority and role responsibilities identified for and communicated to all staff			
• Identification of and access provided to authorized personnel			
Activation of the plan			
• Who can activate the plan, under what circumstances, and how it will be communicated			
• Activation stages established and roles outlined within each stage:			
– Alert—Disaster possible; increased preparedness			
– Stand by—Disaster probable; ready for deployment			
– Call out—Disaster exists; deployment			
– Stand down—Disaster contained; resume normal operations			
Notification process			
• System in place to notify staff of potential or actual disaster			
Response plan by department			
• Standard department operating procedures established to detail how departments will continue to provide service during a disaster			
• Plan developed for how organization will provide supplies and staff in response to external emergencies			
Command structure and center			
• Creation of a command structure and center away from the emergency department			
• Standard operating procedures and chain of command for command center established			
• Equipment and space designated for extra service providers, such as volunteers			
• Coordination with external agencies established			
Security plan to control access and egress			
• Procedure to lock down or minimize access and egress established and tested			
• Plan established to control vehicular and pedestrian traffic			
• Process established to verify credentials of health care and emergency workers from outside the organization who arrive to assist			
Alternate communication systems			
• Alternative communication arrangement made for system failure or overload			
• Organized runner or messenger service in place			
• Communication networks established with local emergency agencies			
Reception of casualties			
• Plan of action in place whereby casualties can be received, identified, triaged, registered, admitted, transferred or transported, and treated.			
Facility evacuation			
• Discharge routine in place to handle large number of patients			
• Staff member responsible for removal and control of patient records and documents identified			
Relocation of patients and staff			
• "Safe" area within the facility identified should other areas become uninhabitable			
• Agreements made with other health care facilities to receive overflow of patients			
• Satellite location of care identified			
• Transportation requirements for movement of staff and patients predetermined and confirmed			
• Sequence of transfer established			
Facility isolation or quarantine			
• Staff members designated for auxiliary power; rationing of food and water; waste and garbage disposal; rest and rotation of staff; rationing of medication and supplies; laundry; and staff and patient morale			
Environment of care and lab assessment			
• Contingency identified for ventilators, IV pumps and poles, suction machines, beds, stretchers, and wheelchairs			
• Medical supplies and linens maintained and readily available			
• Local suppliers of medical equipment and supplies identified and 24-hour contact information available			
Pharmaceuticals			
• Current levels of medications identified			
• Pharmaceutical allocation plan makes provision for prophylaxis of caregiving staff members and their immediate family			
• Other health care facilities that can provide needed pharmaceuticals identified			

Figure 11. JCAHO emergency management checklist (Joint Commission Resources, Inc., 2001).

The culmination of these items for consideration provide a comprehensive list which hospitals can build upon to attain an “all hazards” approach in emergency management. A brief description of the most important planning items is warranted to provide adequate explanation of the level of preparation to consider.

First, it is important to address the regulations and standards that direct action taken by hospitals. OSHA mandates certain actions be taken to provide for the safety of patients and employees of healthcare facilities. An example would be the requirement that training be based upon the duties and responsibilities of each responder for HAZMAT incidents (Sullivan, & Donnelly, 2005). This would apply to any emergency response activity in which employees participate. JCAHO requires any accredited facility to uphold standards, such as the Environment of Care Standard. This standard asks facilities to develop plans and prepare for emergencies adopting an “all hazards” approach, so that, facilities will be ready for any disaster. JCAHO also requires hospitals EMP’s to address the four phases of emergency management (Steinhauer, & Bauer, 2002). Furthermore, hospitals must perform two disaster drills annually, one of which may be a tabletop exercise (Glabman, 2001). These authoritative organizations provide guidelines and mandates, which require that facilities prepare for threats in order to protect everyone within their respective areas of responsibility.

Possibly the single most important consideration for emergency planning is to determine how to protect the healthcare workers within the facility. This begins by ensuring there are appropriate “Lock Down” procedures for the hospital and adequate law enforcement or security guard presence in order to provide for crowd control. Additionally, adequate amounts of PPE appropriate for the threat should be readily available for any employee that may come in contact with a chemical or biological agent. Furthermore, healthcare workers may be hesitant to report to

work when a biological threat or natural disaster occurs, for fear of placing themselves or their families at risk (Bullard, et al., 2002). This should be of extreme importance to administrators because without personnel to staff a hospital, it becomes inoperable. After a large tabletop exercise for bioterrorism participants stated, “Pre-planning for families of healthcare workers was thought to be crucial. Identifying secure locations for families to stay, potentially near the hospital, prioritizing family members for vaccine or prophylaxis, and arranging for childcare facilities were seen as high priorities” (Henning, et al., 2004). Ensuring that employees’ families are taken care of will help alleviate concerns of abandonment and posture the facility to remain viable during emergencies.

Communication is possibly the most important consideration next to taking care of the staff. Almost every emergency exercise drill experiences problems with their communication systems. Whether there were not enough radios available, a lack of coordination between the command center and hospital, or equipment failure, shortcomings with communication hardware and procedure can be a significant problem (Tur-Kaspa, et al., 1999). In real attacks, landlines and cell phones likely will overload immediately, causing phones to become inoperative (Rodoplu, et al., 2004). Therefore, alternate methods of communication need to be explored to ensure the ability to maintain communications with outside hospitals, fire departments, EMS, HAZMAT crews, and government agencies. Some alternatives include; utilizing the hospital emergency area radio network, volunteer amateur radio operators, business handheld radios (similar to family radios), internal phone intercom system, status boards, runners, and posting of digital photos (Rubin, 2004). Others have tried fax networks and email bulk-messaging systems. However, issues such as the inability to open a Word document because of a different version of

Microsoft Word have to be addressed, if these communication options are used (Thompson, 2003).

Surge capacity has been of great concern recently because in today's hospitals it is not economical to operate a facility with empty beds or build larger facilities with empty wings to accommodate surge space. Thus, the excess bed capacity that the United States once experienced no longer exists, which could result in the inability of hospitals to meet increased demand during a natural disaster or terrorist event (Glabman, 2001). The GAO reported that most hospitals did not have sufficient medical equipment and supplies to treat the surge of patients resulting from a bioterrorist attack (GAO, 2003). These concerns were warranted as was made evident from the aftermath of hurricane Katrina, late in 2005. The Joint Commission's (2006) report entitled, *Surge Hospitals: Providing Safe Care in Emergencies*, stated that many hospitals affected by hurricane Katrina had to relocate or surge to sports arenas, veterinary hospitals, and empty retail stores. Hospitals must look outside their facility within the community for space to expand into during disasters and coordinate in advance for support in manning a surge site. Additionally, it is unlikely that the standard levels of care will be able to be provided under the circumstances. Therefore, hospitals should discuss what minimum level of care would be acceptable and publish the standard within the EMP.

An important consideration not to overlook is the provision of mental health services during the disaster response. After the September 11th attacks there was a sharp rise in the number of acute mental health cases, which resulted in almost 20,000 calls and counseling sessions for just one New York area health provider (McGlown, 2004). Not only will patients be affected, but first responders also will have significant mental health needs. This is especially true if the emergency response lasts for an extended period of time. There must be a plan devised

for a work/rest cycle and then provision made for mental health services for these healthcare workers during rest periods (Macintyre, et al., 2000). The military utilizes the Chaplain Corps to help augment mental health workers. Facilities should consider involving local chaplains and pastoral care in emergency management planning for counseling services, as well as provision of Last Rites for unfortunate victims.

Public education and involvement is paramount in creating a viable community response plan. When the public is not consulted about emergency procedures, they may not be willing to follow them. Mark Dubash (2004) states,

Existing terrorism response plans don't account for how people would behave in these situations, according to a study by the Center for the Advancement of Collaborative Strategies in Health at The New York Academy of Medicine. Current plans have been created in a 'top-down' style, telling people what to do in the event of an attack without considering all of the risks and concerns that drive people's actions, the investigators found. The study documents that only two-fifths of the American people would follow instructions to go to a public vaccination site in a smallpox outbreak and only three-fifths would stay inside an undamaged building other than their home after a dirty bomb explosion (pp. 44-45).

A resource that may be useful in educating the public in your area is the CDC fact sheet entitled, "Preparing for a Terrorist Bombing: A Common Sense Approach" and can be found at <http://www.bt.cdc.gov/masstrauma/pdf/preparingterroristbombing.pdf>. This short fact sheet describes what information individuals need to know, what to do, and how to determine whether they need to seek medical attention.

With the danger of HAZMAT incidents on the rise worldwide stemming from industrial based accidents and the increasing threat of terrorism, hospitals need to be prepared to respond. Knowing the types and quantities of PPE to stock is difficult to determine because of the differing opinions concerning what is necessary for chemical, biological, and radiological protection. The Environmental Protection Agency (EPA) has set levels of PPE protection shown in Figure 12.

Levels of Protection

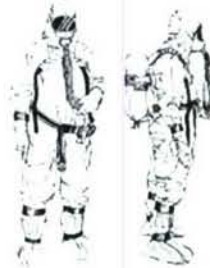
EPA has designated four levels of protection to assist in determining which combinations of respiratory protection and protective clothing should be employed:

Level A protection should be worn when the highest level of respiratory, skin, eye, and mucous membrane protection is needed. It consists of a fully-encapsulated, vapor-tight, chemical-resistant suit, chemical-resistant boots with steel toe and shank, chemical-resistant inner/outer gloves, coveralls, hard hat, and self-contained breathing apparatus (SCBA).



Level A

Level B protection should be selected when the highest level of respiratory protection is needed, but a lesser degree of skin and eye protection is required. It differs from Level A only in that it provides splash protection through use of chemical-resistant clothing (coveralls and long-sleeved jacket, two-piece chemical splash suit, disposable chemical-resistant coveralls, or fully-encapsulated, non-vapor-tight suit and SCBA).



Level B

Level C protection should be selected when the type of airborne substance(s) is known, concentration is measured, criteria for using air-purifying respirators are met, and skin and eye exposures are unlikely. This involves a full facepiece, air-purifying, canister-equipped respirator and chemical-resistant clothing. It provides the same degree of skin protection as Level B, but a lower level of respiratory protection.



Level C

Level D is primarily a work uniform. It provides no respiratory protection and minimal skin protection, and it should not be worn on any site where respiratory or skin hazards exist.



Level D

Figure 12. Levels of PPE adapted from U.S. Department of Health and Human Services, Public Health Service Agency for Toxic Substances and Disease Registry. Managing Hazardous Material Incidents: Volume I. Emergency Medical Services: A Planning Guide for the Management of Contaminated Patients.

In 2005, OSHA released a publication entitled, “OSHA Best Practices for Hospital-Based First Receivers of Victims from Mass Casualty Incidents Involving the Release of Hazardous Substances,” which can be downloaded or printed at

http://www.osha.gov/dts/osta/bestpractices/firstreceivers_hospital.pdf. This document describes in detail the process of hospital decontamination and the equipment that should be used. This new guidance essentially states that hospitals must be prepared to decontaminate victims by protecting their staff with Level B PPE (See Figure 13).

Minimum Personal Protective Equipment (PPE)
for Hospital-based First Receivers of Victims from Mass Casualty Incidents
Involving the Release of Unknown Hazardous Substances

SCOPE AND LIMITATIONS	
This Table applies when:	
▪ The hospital is not the release site.^G ▪ Prerequisite conditions of hospital eligibility are already met (<u>Tables 1 and 2</u>).	▪ The identity of the hazardous substance is unknown.^H
Note: This table is part of, and intended to be used with, the document entitled <i>OSHA Best Practices for Hospital-based First Receivers of Victims from Mass Casualty Incidents Involving the Release of Hazardous Substances</i>.	
ZONE	MINIMUM PPE
Hospital Decontamination Zone^I ▪ All employees in this zone (Includes, but not limited to, any of the following employees: decontamination team members, clinicians, set-up crew, cleanup crew, security staff, and patient tracking clerks.)	▪ Powered air-purifying respirator (PAPR) that provides a protection factor of 1,000.^J The respirator must be NIOSH-approved.^K ▪ Combination 99.97% high-efficiency particulate air (HEPA)/organic vapor/acid gas respirator cartridges (also NIOSH-approved). ▪ Double layer protective gloves.^L ▪ Chemical resistant suit. ▪ Head covering and eye/face protection (if not part of the respirator). ▪ Chemical-protective boots. ▪ Suit openings sealed with tape.
Hospital Post-decontamination Zone^M ▪ All employees in this zone	▪ Normal work clothes and PPE, as necessary, for infection control purposes (e.g., gloves, gown, appropriate respirator)

Figure 13. OSHA's Minimum PPE for Hospital-based First Receivers (OSHA, 2005).

Along with the need for adequate PPE the hospital also has the responsibility to provide an area for patient decontamination (DECON). It does not matter if the facility has little likelihood of facing a terrorist threat, a HAZMAT incident should follow the same procedures. Thus, a terrorist incident is equivalent to a HAZMAT incident, when planning the DECON of patients. The minimum level of DECON consists of having the patients remove their clothing,

which should be bagged and labeled for evidence collection (Siegelson, 2000). The patient decontamination area should have showers for mass DECON, which segregate males and females. Dedicated DECON facilities are preferred, but may not be cost efficient. Some alternatives may be; parking garages with special sprinklers in a dedicated area, HAZMAT DECON tents, or showers affixed to the side of a building. The facility needs to plan for adequate water-heating capability, as the water should be warm, as well as provide a collection system for contaminated water (Dolan, 2002).

One consideration for the EMP should be the provision of emergency medications and immunizations. This should include at least a 24-hour supply stockpiled at the facility and a plan to execute mass immunizations from the strategic national stockpile (Glick, et al., 2004). In recent years, there has been a big emphasis on becoming a needle-less facility, which in a mass immunization effort could become problematic. Therefore, a small stockpile of needles should be on hand for emergency operations (Young, 2005). Furthermore, medications and immunizations indicated for children should be dosed accordingly (Thompson, 2003). Careful planning with the local health department and other healthcare agencies will help to identify appropriate plans and procedures for the community.

Just as with pharmacy issues, maintaining adequate levels of supply for the rest of the facility remain vitally important during emergency operations. Memoranda of understanding (MOU's) need to be in place with all essential vendors to ensure the seamless continuity of deliveries during emergencies. Supplies, including food and water, should be stocked to last at least 24 hours. It is essential that the hospital maintain the ability to be self-sufficient for at least 24 hours without re-supply, because it may take time for outside agencies to provide relief (Steinhauer, & Bauer, 2002). Additionally, local mass transportation options will be affected and

may be used for other community emergency purposes. The hospital must plan an alternate method for evacuation or acquire MOU's to ensure usage by the facility (Glick, et al., 2004).

The facility's power plant requirements, which include power, fuel, and water supplies, are just as important as other logistical concerns. JCAHO mandates that backup generators start up within 60 seconds. However, if they are damaged by a disaster what will the hospital do? Alternate plans to provide power are essential. Several solutions include; a contract with an out of town vendor for a tractor-trailer based generator, rental contracts with local equipment supply companies, and using Uninterruptible Power Supply (UPS) for computers. Moreover, if the water becomes contaminated, the hospital should have contracts with local suppliers, such as swimming pool fillers, water trucks, and the fire department, for emergency water supply. The staff should utilize antiseptic hand rinse solutions or moist towelettes, when water is not available for hand washing (White, 2002).

Essential to the success of any emergency response plan is coordination with outside agencies to help support the facility's response. This is especially true when working with local and state agencies. JCAHO recommends hospitals plan cooperatively with other organizations within the community, which can be accomplished through community collaboratives or local emergency response teams. The ability to respond immediately to any threat requires public and private partnerships between hospital personnel, public health department, fire department, law enforcement, mental health professionals, laboratory services, local pharmacies, and community volunteers (Glick, et al., 2004). Additionally, local HAZMAT teams can be utilized at the emergency department to augment hospital staff with DECON of patients (Siegelson, 2000). Not only is the local community response plan critical to success, but it also may be more cost effective by pooling resources together to answer the threat (Scharoun, et al., 2002). When

dealing with state agencies the hospital CEO should use his or her political influence to ensure that financial support is funneled through the local health department in order to augment a facility's response capability. Planning with local and state governments is vital in implementing the current procedure of first, initiating the local response, then notifying the state, and finally federal authorities concerning the event (Glabman, 2001). The type and size of the emergency will determine how quickly the next level of support intervenes. After the failed response to hurricane Katrina, requests may move more quickly from the local level to the federal level.

Training

Planning to train employees in emergency management should be a top priority. Particularly those who will be involved with patient DECON activities. When looking for training options, a facility will be confronted with numerous choices. However, lack of guidelines and quality control measures may make it difficult to choose the best training program. The most common training program among hospitals is HEICS (Rubin, 2004). Additionally, hospital responders must have training in chemical and biological illness identification, because triage personnel may be the key to stopping the spread of the agent or organism within the facility. When employees suspect a bioterrorism case, they need to know whom to contact in the community and state public health agencies (Henning, et al., 2004). Training will help employees feel more confident to fulfill emergency response roles when disaster strikes.

Exercises

Testing the hospital's preparedness is essential to maintaining an "all hazards" approach to emergency management. Not only is it mandated for JCAHO accredited health centers, but also periodic drills and exercises help employees retain valuable skills as first responders. It is

much better to make mistakes and discover shortfalls during training and disaster drills than to discover them when an emergency occurs. JCAHO allows two types of drills. The least expensive and resource intensive drill is the tabletop exercise, which allows the participant to think through a scenario and act as necessary. Henning et al., (2004) performed a survey, which studied a large tabletop exercise and found that 79% of respondents stated the tabletop exercise was extremely or very useful (p. 152). The second type of drill is the traditional hands-on emergency exercise usually encompassing some type of MASCAL scenario. It is important when planning an exercise to include security personnel, so that they can receive valuable hands on experience (Klaas, 2005). Reoccurring feedback following many exercises is the need for increased funding to make the drills more realistic (Rubin, 2004). Since many hospitals have budget problems, increasing exercise funding becomes problematic. However, the Department of Homeland Security has compiled information on available emergency management grants found at <http://www.dhs.gov/dhspublic/display?theme=18>.

All of these planning techniques, coupled with training and testing through emergency drills represent the preparedness phase of emergency management. As long as hospitals prepare as best they can, they will be ready to respond when an actual emergency occurs. The next phase of emergency management is the response phase. The success of this phase will depend on how well the hospital follows their emergency management plan, which in turn depends on how familiar individuals are with the plan and the training they have received.

Response Phase

The main part of the response phase is the actual performance of incident management during the emergency. As stated before, the most widely used template for hospital incident management is the HEICS system, which is adapted from the Incident Command System. At the

very minimum, the hospital needs a well-defined chain of command (COC) to direct emergency management efforts (Steinhauer, & Bauer, 2002). A mistake often made by first responders is the desire to rush into the incident scene without taking precautions, which would include clearing the scene for safety and donning their PPE (Rodoplu, et al., 2004). Until the scene has been designated clear of chemical and HAZMAT substances, the assumption must be that it is contaminated. Moreover, recent terrorist events suggest first responders have become soft terrorist targets. Secondary IED's may be placed near the incident scene or at the ED entrance to instill terror among those attempting to help the victims of the initial attack (Vassallo, et al., 1997).

At the same time the first responders arrive on the scene, initial reports of the incident will begin to trickle into the hospital. As soon as the reports come in, the hospital needs to initiate its Emergency Operations Center. If there are any indications of chemical or biological agents from the attack, the hospital needs to lockdown the facility and cease all non-essential activities. Security needs to post guards at all access points and direct vehicle traffic at the entrance to the campus. The guards need to have training to implement crowd control procedures, as a pandemic flu or bioterrorist attack could cause civil unrest due to people trying to access limited stockpiles of immunizations or medications (Klaas, 2005). The hospital should consider having an official agreement with local law enforcement to help augment security services at the facility during emergency operations (Rubin, 2004).

Another important consideration in incident management is the triage of the injured who are arriving from the scene of the disaster. "The goal of triage is to identify that minority of critically injured casualties who require immediate treatment in order to render that treatment as soon as possible" (Frykberg, & Tepas, 1988). A triage officer should be in charge of the process

with no other duties to jeopardize the outcome of casualty management. The triage area should be kept open for several hours after the initial incident with minimal staffing as casualties may trickle in. Additionally, patient administration needs to be present and provide a mechanism to track the patient from triage to transfer or release (Vassallo, et al., 1997). Furthermore, mental health providers should be present to help casualties and staff with acute mental illness symptoms stemming from the event.

In the event of a chemical or HAZMAT incident, the casualties will need to be decontaminated prior to entering the facility for definitive care. For efficient patient DECON, the area needs to be set up to move casualties from the DECON site to the ED (See Figure 14). As previously discussed, all responders inside the DECON site must be protected with level B PPE. During DECON procedures, clothes are removed and bagged with the patient's information. The clothing is evidence and hospitals will be held responsible for proper collection, which may then be used in ensuing investigations. Furthermore, hospitals near medical or nursing schools can set up agreements to augment the facility staff during manpower extensive activities such as patient DECON (Glick, et al., 2004). Medical personnel from around the community may volunteer to help, thus the leadership needs to plan how the hospital will grant emergency credentials (Henning, et al., 2004).

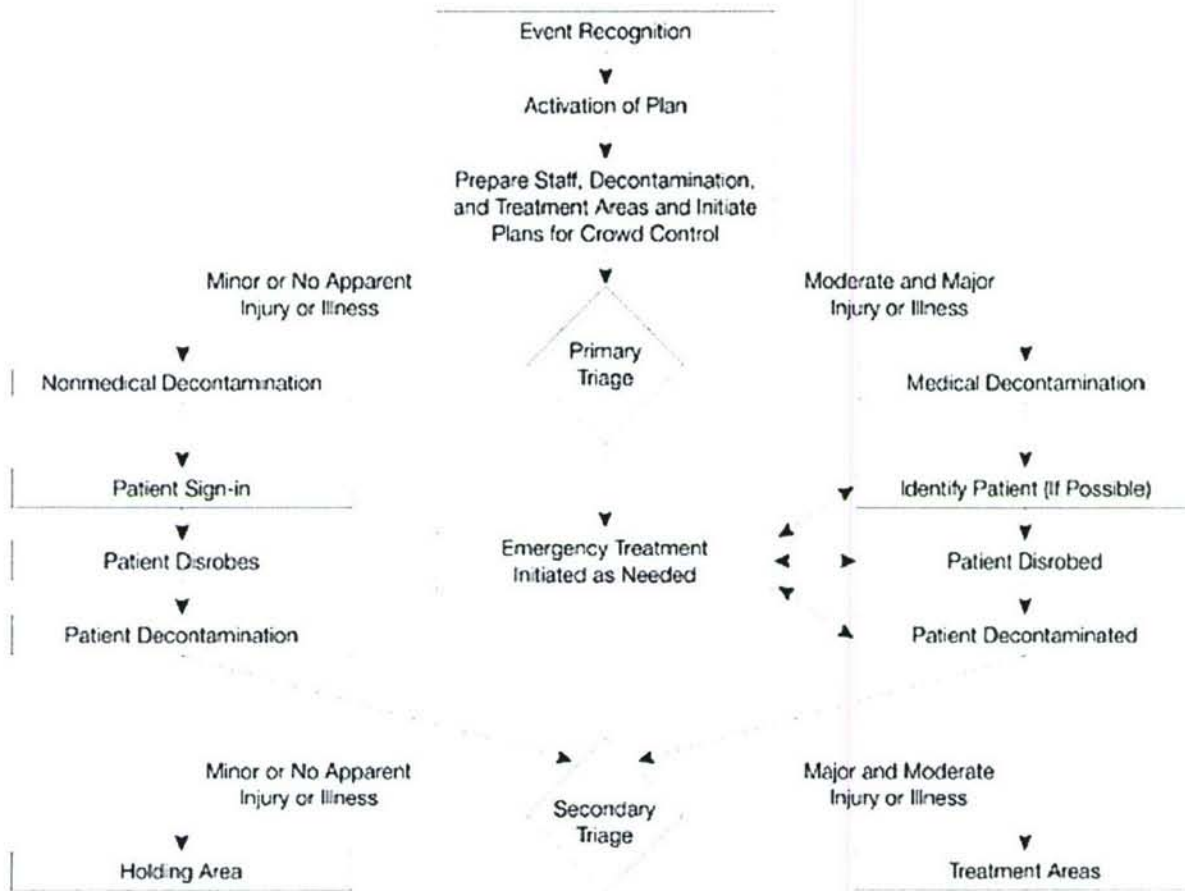


Figure 14. Healthcare facility response plan for chemical or biological weapons release (Macintyre, et al., 2000).

Incident management is the true test of a hospital's preparedness to respond to emergencies. How well the hospital prepares for and takes steps to mitigate hazards, will determine the quality of emergency response the facility provides. Healthcare facilities cannot plan for everything that will actually occur during a disaster, but they can limit problems by addressing the four phases of emergency management. The recovery phase may be the most important for a hospital because if the facility cannot return to normal operations within a short period of time, the financial shortfall could bankrupt the organization.

Recovery Phase

Immediately following a disaster, the recovery process should already be in place to restore normal operations as quickly as possible. Thus, pre-coordination and contracts with vendors are needed to ensure a seamless transition from the response phase to the recovery phase (Steinhauer, & Bauer, 2002). Jerry Mothershead, a physician advisor at Battelle Memorial Institute in Hampton, Virginia, suggests the following considerations in recovery planning (2004, p. 71):

Short-Term Recovery

- Obtaining temporary food, water, and housing
- Maintaining medical services
- Restoring power, water, communications, etc.
- Temporarily closing roads and rerouting traffic
- Clearing downed trees
- Repairing public / private buildings and homes
- Restoring order and ensuring law enforcement; establishing safety and security

Long-Term Recovery

- Demolishing damaged buildings and homes
- Removing massive amounts of debris
- Restoring lifeline systems (critical infrastructure components)
- Instituting major reconstruction programs
- Revising building and land-use codes

- Solving cash-flow and economic problems
- Dealing with business failures or closures and high unemployment
- Addressing political issues

If there is any damage to the hospital, operations may need to move to an alternate site. The facility needs to maintain several options for off-site housing of patients. The extent of the disaster will determine which course the hospital should pursue to take care of the patients in the area. If there are suitable, undamaged locations nearby that will house patients, then equipment and supplies will need to be transferred, leased, or borrowed to accommodate the movement of operations (Mothershead, 2004).

If the damage is more widespread and beyond the capability of the local response, then political influence should be exerted to obtain a mobile hospital complete with equipment and staff. The Health Resources and Services Administration (HRSA) provides funding for emergency preparedness. This was made evident in the recent aftermath of hurricane Katrina. The HRSA provided funding to set up a mobile hospital that treated over 7,000 local residents in Mississippi after hurricane Katrina and was the only hospital operating in Hancock County during that time (HRSA, 2005). The Army Reserves also have assets that can assist in providing temporary medical facilities. In essence, the recovery phase also requires prior planning to ensure an organization will survive a disaster that can be economically devastating to an area and business.

Summary

Current sources reveal terrorists are targeting hospitals and first responders in an unprecedented approach to instill terror and reduce lifesaving capabilities of their enemies (See Appendix A). Security of our healthcare facilities is now a top priority for executives.

Additionally, hospitals are being asked to prepare to respond to mass casualty events resulting from terrorist attacks and natural disasters such as hurricane Katrina. These concerns are creating the need for more research and resources to be available for hospitals to utilize in preparing for these threats.

This study represents a comprehensive summary of current literature resulting in the development of several tools assisting hospitals to evaluate and address security issues within their facilities. Furthermore, security concerns occur in each phase of emergency management and specific items were presented within each phase to adequately address the issue. The four phases of emergency management exist to facilitate an organizations preparedness to respond to natural and manmade disasters. The mitigation phase encompasses hazard identification specific to the facility, which can then be utilized to create a hazard vulnerability analysis. The HVA fulfills the “all hazard” approach to emergency management that JCAHO accredited facilities must follow. The HVA provides hospitals with a listing of most probable threats, which then may be used to establish measures to mitigate them. Ensuring health centers have adequate security is key to help mitigate most crime and terrorist activity on campus. Additionally, technologies such as CCTV, card access systems, biometrics, chemical and radiological identification devices, and blast resistant materials help to harden a facility against terrorism.

Classic emergency management focuses on the preparedness and response phases, with which most professionals have some experience. The preparedness phase consists of a plan prescribing how the facility and personnel will react to hazards predetermined by the HVA. Personnel must be trained in whatever position they hold so they can perform as expected. Periodic testing through emergency exercises will help prepare the hospital and staff for real emergencies by spotlighting weaknesses and refining processes. The response phase is

highlighted by incident management, which is usually based upon HEICS. Finally, the recovery phase addresses the planning necessary for restoring normal operations to the hospital, which will depend on the type and magnitude of the disaster.

I recommend hospitals independently conduct a HVA and then utilize the security assessment checklist and terrorism mitigation matrix to lessen any threat facing the facility. Additionally, the success of a hospital's emergency management program is the responsibility of the CEO and board of directors. If they make the program a priority, it will be successful. If the hospital and staff are prepared, there will be no need to fear the threats that oppose them.

References

- About, Inc. (2005). A concise history of terrorism. Retrieved October 11, 2005, from http://terrorism.about.com/od/historyofterrorism/a/concisehistory_p.htm
- AP. (2004, August 27). VA hospitals in Qaeda's sights. *CBS News*. Retrieved October 6, 2005, from <http://www.cbsnews.com/stories/2004/08/27/terror/printables638934.shtml>
- Arterburn, T. (2002). What hospital security should be doing now to better prepare for future activity. *Journal of Healthcare Protection Management*, 18(1), 6-14.
- Brown, D. (2005, April 22). Fake hospital inspectors probed. *Washington Post*. Retrieved October 6, 2005, from <http://www.washingtonpost.com/ac2/wp-dyn/A7680-2005Apr21?language=printer>
- Bullard, T., Strack, G., & Scharoun K. (2002). Emergency department security: A call for reassessment. *Health Care Manager*, 21(1), 65-73.
- CFR. (2005). 28 C.F.R. Section 0.85. Retrieved October 13, 2005, from C.F.R. Online via GPO Access: <http://frwebgate1.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=192253291751+10+0+0&WASAction=retrieve>
- Committee on Government Reform. (2004). Letter to Secretary of State, Colin Powell. Retrieved March 29, 2006, from <http://www.democrats.reform.house.gov/Documents/20040608080152-97773.pdf>
- County Profiles: Germany (2005). Terrorism Research Center. Retrieved October 4, 2005, from <http://www.terrorism.com/modules.php?op=modload&name=Countries&file=index&view=91>
- Department of the Army. (1994). *Leader's manual for combat stress control* (FM 22-51, 9-4). Washington, DC: Author.

- Department of Defense. (2003). *Department of Defense Directive 2000.12*. Retrieved January 12, 2006, from <http://www.dtic.mil/whs/directives/corres/pdf2/d200012p.pdf>
- Department of Health and Human Services. (2002). *Guidance for protecting building environments from airborne chemical, biological, or radiological attacks*. Retrieved October 15, 2005 from www.cdc.gov/niosh/bldvent/2002-139.html
- Department of Homeland Security. (2003). *The national strategy for the protection of critical infrastructures and key assets*. Retrieved January 26, 2006, from http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf
- Dolan, K. (2002). Suspicious powder is everywhere. *Journal of Emergency Nursing*, 28(2), 143-144.
- Dubash, M. (2004). Terrorism response plans will not protect many Americans, new study finds. *Journal of Environmental Health*, 67(5), 44-45.
- ECIS. (2003). Personal accident insurance – definitions. Retrieved October 13, 2005, from <http://www.ecis.org/finance/paisdefin.htm>
- FEMA. (n.d.). Backgrounder: Terrorism. Retrieved October 11, 2005, from www.fema.gov/pdf/hazards/terrbk.pdf
- FEMA. (2004). Building design for homeland security Retrieved February 22, 2006, from http://www.fema.gov/pdf/fima/155/e155_sm.pdf
- Frykberg, E., & Tepas, J. (1988). Terrorist bombings. Lessons learned from Belfast to Beirut. *Annals of Surgery*, 208(5), 569-76.
- Ganor, B. (2001). Defining terrorism: Is one man's terrorist another man's freedom fighter? Retrieved October 11, 2005, from <http://ict.org.il/articles/define.htm#15>
- Glabman, M. (2001). Bioterrorism: The silent killer. *Trustee*, 54(10), 29-33.

- Glass, G. V. (1976). Primary, secondary, and meta-analysis of research. *Educational Researcher*, 5, 3-8.
- Glick, D., Jerome-D'Emilia, B., Nolan, M., Burke, P. (2004). Emergency preparedness one community's response. *Family & Community Health*, 27(3), 266-273.
- Gonzalez, J. (2002). Delivering security in today's new threat environments. *Journal of Healthcare Protection Management*, 18(2), 35-38.
- Grigsby, J. (n.d.). Disaster recovery plans – Now more than ever. *The Receivables Report*, 17(4), 11-12.
- Henning, K., Brennen, P., Hoegg, C., O'Rourke, E., Dyer, B., Grace, T. (2004). Health system preparedness for bioterrorism: Bringing the tabletop to the hospital. *Infection Control and Hospital Epidemiology*, 25(2), 146-155.
- Hodgson, K. (2003, March). First defense: Using design elements to strengthen security efforts. *Health Facilities Management*, 16(3), 16-20, 22, 24-25.
- Health Resources & Services Administration (HRSA). (2005). HRSA hospital preparedness grantee in N.C. takes mobile hospital, staff to Miss. to help hurricane victims. Retrieved January 17, 2006, from <ftp://ftp.hrsa.gov/katrina/updatehrsa1011.pdf>
- Joint Commission Resources, Inc. (2001). Emergency management in the new millennium. *Perspectives*, 21(12), 1-23.
- Joint Commission Resources, Inc. (2005). *Hospital Accreditation Standards 2005*. U.S.A.: Author.
- Joint Commission Resources, Inc. (2006). *Surge hospitals: Providing safe care in emergencies*. Retrieved March 9, 2006, from http://www.jcaho.org/about+us/public+policy+initiatives/surge_hospital.pdf

- Klaas, M. (2005, January). Security stat!. *Health Facilities Management*, 18(1), 22-26.
- Klein, S. (2003, May 12). Security check. *Crain's Chicago Business*, 26, 13-14.
- Landstuhl Regional Medical Center (2005a). LRMC history. Retrieved October 3, 2005, from <http://www.landstuhl.healthcare.hqusareur.army.mil/resources/history.aspx>
- Lee, R. (2006). The history guy: The Afghan Civil War (1978-Present). Retrieved March 29, 2006, from http://www.historyguy.com/afghan_civil_war.html
- Leonidas, T., & O'Donnell, J. (2005, July). High tech sentinels. *Health Facilities Management*, 18(7), 25-30.
- Long, R. & Pry, W. (2002, May). Hospital security a top issue says survey. *Healthcare Benchmarks*, 9(5), 55-56.
- Luizzo, A. & Scaglione, B. (2004). How has hospital security changed since 9/11?. *Journal of Healthcare Protection Management*, 20(2), 44-48.
- Macintyre, A., Christopher, G., Eitzen, E., Gum, R., Weir, S., DeAtley, C., et al. (2000). Weapons of mass destruction events with contaminated casualties: Effective planning for health care facilities. *The Journal of the American Medical Association*, 283(2), 242-249.
- McAdams, K., Russell, H., & Walukewicz, C. (2004). Gangstas – not in my hospital!. *Nursing*, 32(9), 32hn1-32hn4.
- McGlown, K. (2004). Preparing your healthcare facility for disaster. In K. J. McGlown (Ed.), *Terrorism and disaster management* (pp. 3 – 18). Chicago, IL: Health Administration Press.
- Mothershead, J. (2004). The new threat: Weapons of mass effect. In K. J. McGlown (Ed.), *Terrorism and disaster management* (pp. 27 – 48). Chicago, IL: Health Administration Press.

- Moss, B. (2002, July). Puzzled by security?. *Health Facilities Management*, 15(7), 17-21.
- Nash, J. (1998). *Terrorism in the 20th Century*. New York, New York: M. Evans and Company, Inc.
- National Alliance of Gang Investigators Associations (2005). 2005 National gang threat assessment. Retrieved February 15, 2006, from http://www.ojp.usdoj.gov/BJA/what/2005_threat_assesment.pdf.
- NBC news services (2005, September 14). Nursing home owners charged in storm deaths. *NBC News*. Retrieved January 17, 2006, from <http://www.msnbc.msn.com/id/9337631>
- Noble, S. (2002, May). As in today's world, in today's hospital, security takes many forms. *Healthcare Purchasing News*, Retrieved January 24, 2006, from <http://www.hpnonline.com/inside/2002-05/0502cover.html>
- Occupational Safety and Health Administration (OSHA). (2005). OSHA best practices for hospital-based first receivers of victims from mass casualty incidents involving the release of hazardous substances, Retrieved March 10, 2006, from http://www.osha.gov/dts/osta/bestpractices/firstreceivers_hospital.html
- Pietrzak, M. (2004). Threat mitigation in hospital design. *Hospital Engineering & Facilities Management*. Retrieved February 21, 2006, from <http://www.touchbriefings.com/download.cfm?fileID=1847>
- Ridge, T. (2002, April 8). Director Ridge speaks at American Hospital Association meeting. *Whitehouse.gov*. Retrieved September 23, 2005, from <http://www.whitehouse.gov/news/releases/2002/04/print/20020408-5.html>

- Rodoplu, U., Arnold, J., Tokyay, R., Ersoy, G., Cetiner, S., & Yucel, T. (2004). Mass-casualty terrorist bombings in Istanbul, Turkey, November 2003: Report of the events and the prehospital emergency response. *Prehospital and Disaster Medicine*, 19(2), 133-145.
- Rubin, J. (2004). Recurring pitfalls in hospital preparedness and response. *Journal of Homeland Security*. Retrieved October 4, 2005, from <http://www.homelandsecurity.org/newjournal/articles/rubin.html>
- Sarnese, P. (1997). Assessing security in the emergency department: An overview. *Journal of Emergency Nursing*, 23(1), 23-26.
- Seper, J. (2005, June 9). California man, son linked to al Qaeda. *The Washington Times*. Retrieved October 6, 2005, from <http://washingtontimes.com/functions/print.php?StoryID=20050609-120317-3781r>
- Sharoun, K., Caulil, K., & Liberman, A., (2002). Bioterrorism vs. health security – Crafting a plan of preparedness. *Health Care Manager*, 21(1), 74-92.
- Shinkman, R. (2003). Locked down: Preserving hospital security. *Healthcare Leadership and Management Report*, 11(9), 9-13.
- Shughart II, William F. (2005). An analytical history of terrorism, 1945-2000. Unpublished manuscript, University of Mississippi. Retrieved October 11, 2005, from <http://home.olemiss.edu/~shughart/Analytical%20History%20of%20Terrorism.pdf>
- Siegelson, H. (2000). When terrorists strike: Are you prepared? *Materials Management in Health Care*, 9(1), 22-28.
- Simon, H., Khan, N., & Delgado, C. (2003). Weapons detection at two urban hospitals. *Pediatric Emergency Care*, 19(4), 248-251.

State of Delaware. (2005). The history of terrorism: More than 200 years of development.

Retrieved August 23, 2005, from <http://www.state.de.us/cjc/terrorism/history.shtml>

Steinhauer, R., & Bauer, J. (2002). The emergency management plan. *RN*, 65(6), 40-46.

Sullivan, M., & Donnelly, B. (2005). Emergency department response to terrorism. *Topics in Emergency Medicine*, 27(1), 50-77.

Thompson, C. (2003). Illinois hospital pharmacies check their emergency preparedness.

American Journal of Health-System Pharmacy, 60, 1299-1300.

Tur-Kaspa, I., Lev, E., Hendler, I., Siebner, R., Shapira, Y., & Shemer, J. (1999). Preparing hospitals for toxicological mass casualties events. *Critical Care Medicine*, 27(5), 1004-1008.

U.S. Attorney's Office District of Connecticut. (2003). Antiterrorism Advisory Council.

Retrieved October 11, 2005, from <http://www.usdoj.gov/usao/ct/attf.html>

U.S. Code. (2002, January). Title 22 Foreign relations and intercourse (22USC2656f). Retrieved

October 13, 2005, from U.S. Code Online via GPO Access:

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+22USC2656f

U.S. Congressional Record. (2005). *Statement of Senator Diane Feinstein "The response to hurricane Katrina"*. Retrieved January 17, 2006, from

<http://feinstein.senate.gov/05speeches/cr-katrina.pdf>

U.S. Department of Health and Human Services (DHHS), Public Health Service Agency for Toxic Substances and Disease Registry. (2001). Managing hazardous material incidents: Volume I. Emergency medical services: A planning guide for the management of

- contaminated patients. Retrieved March 10, 2006, from <http://www.atsdr.cdc.gov/mhmi-v1-2.pdf>
- U.S. Department of Justice. (2002). Federal Bureau of Investigation report on terrorism 2000/2001 (FBI Pub# 0308). Retrieved October 11, 2005, from http://www.fbi.gov/publications/terror/terror2000_2001.pdf
- U.S. Department of State. (2004, June). Patterns of global terrorism 2003. Retrieved October 11, 2005, from <http://www.state.gov/s/ct/rls/pgtrpt/2003/c12153.htm>
- U.S. Department of Veterans Affairs. (2006). The four phases of comprehensive emergency management. Retrieved January 12, 2006, from http://www1.va.gov/emshg/apps/emp/emp/figure_2_1_four_phases.htm
- U.S. General Accounting Office (GAO). (2003). Hospital preparedness: Most urban hospitals have emergency plans but lack certain capacities for bioterrorism response (GAO Publication No. 03-924). Rockville, MD: Author.
- Vassallo, D., Taylor, J., Aldington, D., & Finnegan, A. (1997). Shattered illusions – The Thiepval barracks bombing. *Journal of the Royal Army Medical Corps*, 143(1), 5-11.
- Vogt, B., & Sorenson, J. (2004). Protecting the healthcare population and facility. In K. J. McGlown (Ed.), *Terrorism and disaster management* (pp. 99-124). Chicago, IL: Health Administration Press.
- White, D. (2002). A terrorism response plan for hospital security and safety officers. *Journal of Healthcare Protection Management*, 18(1), 15-23.
- Young, D. (2005). States, hospital learn emergency-preparedness lessons in TOPOFF 3. *American Journal of Health System Pharmacy*, 62, 1000-1004.

Appendix A

Chronological Listing of Terrorism Conducted Against Hospitals Since 2001

2001 Attacks

26 May – Philippines

In Palawan, the Abu Sayaa Group (ASG) kidnapped 20 persons including three US citizens and 17 Filipinos from a beach resort and took them to Basilan Island in Sulu Archipelago, according to press reports. On 31 May, three captives were released unharmed. On 2 June, the kidnappers, with their hostages in tow, raided a hospital and church in Lamitan, Basilan, temporarily taking 200 persons hostage. They managed to escape from an ensuing gun battle with Philippine military forces and added five hospital employees to their group of hostages. On 4 June, the ASG released two female hostages after ransom was paid, according to press reports. Three more Philippine hostages were released on 16 June. On 26 June, two more Philippine civilians were taken hostage. In June, the ASG beheaded one of the US hostages. At year's end, two of the 20 original hostages (both US citizens) and one Filipino from the Lamitan hospital remained captive (US Department of State, 2002, p. 77).

8 June – Columbia

In Florida, a Spaniard was kidnapped after leaving the hospital where she worked, according to press reports. On 7 July, the Spaniard was released and left on the mountains in southwestern Colombia. Motives for the kidnapping were unclear, no ransom was collected, and no one claimed responsibility. Authorities found that her captives, a group of guerillas from the 19 April Movement (M-19), also referred to as the Jaime Bateman Canyon Movement, were responsible (US Department of State, 2002, p. 78).

2002 Attacks

May – Liberia

Phebe hospital in Gbarnga, was attacked and sacked in May 02. A month later since the hospitals evacuation, staff is beginning to return and prepare the hospital for operation. Most of the equipment and supplies were taken and the hospital needs aid to reopen (Lutheran World Relief, 2002).

9 August – Pakistan

For the second time this week, terrorists have attacked a Christian institution in Pakistan. On Friday morning (Aug. 9), three men lobbed grenades at hospital workers as they left the morning chapel service at the Christian (Presbyterian) Hospital in Taxila, near the Pakistani capital of Islamabad. Presbyterian Church (USA) officials here confirmed wire service reports that four people were killed - three nurses at the hospital and one of the attackers. The other two assailants are still at large, according to Pakistani police. The blasts also injured more than two dozen people, most of whom were cut by flying glass, according to the hospital's chief administrator, Ernest Lall...security guards delayed the attackers when they tried to enter the hospital campus, preventing an attack on the staff while it was gathered in the chapel. He said the loss of life in that case might have been much greater (Van Marter, 2002).

30 December – Yemen

Yemeni officials said three Americans were killed yesterday at a Baptist missionary hospital in central Yemen by a man apparently belonging to a small cell that planned to victimize both Westerners and secular Yemenis. A fourth American was seriously

wounded in the attack, which occurred yesterday after the assailant, identified by the Yemeni new agency, Saba, as Abed Abdul-Razak al-Kamil, sneaked a semiautomatic rifle into the hospital under his coat. Saba reported that Mr. Kamil, 30, surrendered to authorities and was arrested after the incident, the latest in a series of Islamic militant attacks against easily accessible American targets in the region... Yemen has been the site of frequent terrorist attacks linked to Al Qaeda (MacFARQUAR, 2002, Section A, p.1).

2003 Attacks

August 1 – Chechnya

A powerful vehicle bomb blast destroyed a Russian military hospital near the breakaway republic of Chechnya Friday, killing at least 50 and wounding some 70 others. "About 6:58 pm Moscow time, a [heavy truck] loaded with explosives rammed through the gate of the hospital and exploded near the hospital's management building," a spokesman for the hospital told the Interfax news agency in the wake of Friday's blast. The four-story hospital is located in the North Ossetia town of Mozdok, considered the headquarters for Russian forces combating separatist fighters in neighboring Chechnya (PBS, 2003, August 4).

September 11 – Liberia

In a disturbing development, 20 armed government militia this week marched into Phebe Hospital in Salala, held the staff at gunpoint, and ransacked the premises. Medical supplies and communications equipment were stolen. Although accurate information on the status of the patients is scarce, two have reportedly died. The whereabouts of the remaining 50 patients is unknown (UN Press Release, 2003).

December 30 – Germany

Hamburg - German authorities said on Tuesday they had uncovered plans by suspected Islamic extremists to launch a suicide car-bomb attack on a military hospital in the northern city of Hamburg. Dirk Nockemann, the Hamburg senator responsible for internal affairs, said the militant Islamic group, Ansar al-Islam, which is alleged to have links to al-Qaeda, was likely to be behind the plans. Citing United States intelligence sources, he said members of the group had planned a suicide-bomb attack, while an alternative target was the major US Rhein-Main air base in central Germany... Fallak said there was no clear evidence of when the attack was planned, but that it involved extremists "from Europe" but outside Hamburg. In a statement, police said that security sources had passed on "concrete evidence about people who want to carry out attacks on the hospital with a car bomb". "The potential perpetrators are understood to come from Islamic terrorist circles."...US authorities believe Ansar al-Islam has links to Al-Qaeda, the extremist network responsible for the September 11 2001 attacks in the United States. The group's stronghold in northern Iraq was devastated by US air strikes in early April during the US invasion of Iraq. However, US commanders have said Ansar al-Islam has made a strong comeback, infiltrating Iraq from Iran and setting up operations in the Baghdad area. German intelligence services believe about 100 Ansar al-Islam militants are in Germany, mainly in the south of the country (News24, 2003, December 30).

2004 Attacks

July 26 – India

On 26 July 2004, in Baramulla Town, Kashmir, India, Islamic militants threw a grenade at a hospital where Border Security Forces had been admitted for treatment, killing one person and injuring 30 others. No group claimed responsibility (National Counterterrorism Center, 2005).

August 5 – Najaf, Iraq

Najaf's general hospital, attacked by rockets in the morning - killing a doctor and seriously wounding four other staff members - said seven people died in the fighting and another 32 were admitted with injuries (DAWN, 2004, August 6).

September 21 – India

On 21 September 2004, in Surankote, Poonch District, Kashmir, India, Islamic militants threw a grenade at a hospital, wounding two civilians. No group claimed responsibility (National Counterterrorism Center, 2005).

November 9

Car bombs at two Baghdad churches and outside a hospital treating the victims of those attacks killed at least eight people and wounded dozens overnight as a wave of blasts struck the Iraqi capital...Victims from both blasts, some carried by injured friends or relatives in torn and bloodstained clothes, were rushed to Yarmouk hospital. A doctor said at least three people had been killed and 40 injured...at least 13 people were killed

and about 60 injured when a car bomb exploded outside the emergency unit of one of Baghdad's main hospitals late Monday (Ireland, 2004, November 9).

2005 Attacks

January 20 – Mosul, Iraq

Iraqi Security Forces guarding the Al Salam Hospital in eastern Mosul, Iraq, held off an insurgent attack today, Multinational Force Iraq officials reported. Doctors, Staff, and patients fled the hospital because of the attack, and no injuries were reported (American Forces Information Service, Jan 20).

February 7 – Mosul, Iraq

Suicide bomb attacks outside a hospital and a police station killed 27 Iraqis early Monday, officials said. In Mosul, a suicide bomber outside Jumhuriya Hospital summoned a group of policemen to him and detonated the bomb killing 12 and wounding four, officials and witnesses said. "I heard an explosion. When I went to check, I saw bodies everywhere," Tahseen Ali Mahmoud al-Obeidi, hospital director, told The Associated Press. About a half-hour later at 3 a.m., an explosives-laden taxi blew up, killing 15 people, police said (CNN, 2005, February 7).

February 12 – Musayyib, Iraq

A blast outside a hospital killed at least 17 people and injured about 25 more in the town of Musayyib, about 70 km (45 miles) south of Baghdad (BBC, 2005, February 12).

May – Iraq

Earlier this month, violence peaked when terrorists detonated a vehicle-borne improvised explosive device next to the Haditha hospital. In the aftermath of the ensuing firefight, coalition forces discovered that terrorists had physically taken over portions of the hospital and constructed bunkered fighting positions. The terrorists caused major structural damage to the hospital, placing significant strain on health care in the Haditha region, according to U.S. officials (American Forces Information Service, 2005, May 30).

June 4 – Baghdad, Iraq

In north-central Baghdad, Iraqi police responded quickly and established order June 3 after a mid-afternoon mortar attack failed to cause significant damage when a round struck a hospital's respiratory center, officials said. Shortly after 2 p.m., terrorists fired multiple mortar rounds at the respiratory center in the Baghdad Medical City Complex. One mortar round exploded on the respiratory center and another round exploded on the roof of a nearby house, officials said. The terrorists then sprayed the hospital with automatic rifle fire, killing one local citizen (American Forces Information Service, 2005, June 4).

June 26 – Mosul, Iraq

A third attacker strapped with explosives walked into Mosul's Jumhuri Teaching Hospital in the afternoon and blew himself up in a room used by police guarding the facility, killing five policemen. An Associated Press reporter was outside the hospital when the explosion occurred, blowing a hole in a side of the building and injuring some police officers outside. Smoke then began pouring out of the hole, followed by flames.

Inside, dead police officers who apparently had been sleeping were sprawled in their underwear, their bodies and the walls peppered with ball bearings...Abu Musab al-Zarqawi's Al Qaeda in Iraq claimed responsibility for the attacks in Mosul (FOXNews, 2005, June 26).

July 3 – Warangal, India

One person was killed and 10 others, including five policemen, were injured when a powerful bomb went off at the outpatient ward in Mahatma Gandhi Memorial (MGM) Hospital here on Saturday. The bomb was placed in a Tiffin box and left under cement benches in the busy OP ward (The Hindu, 2005, July 3).

July 11 – Baghdad, Iraq

Iraqi soldiers stopped three terrorist attacks against a water plant, a military recruiting drive, and a hospital July 11, all around Baghdad. The third incident occurred just before noon, when a citizen told Iraqi soldiers he'd seen a car bomb parked near a hospital in south Baghdad. They secured the site and called in explosives experts to investigate. The team found a white car with wires running from the transmission to two batteries. It also found a bomb near the hospital consisting of four mortar rounds. The team safely removed the car bomb and munitions from the site (American Forces Information Service, 2005, July 13).

August 17 – Baghdad, Iraq

The first part of the attack involved a car bomb that detonated at a bus terminal in downtown Baghdad at 7:50 a.m. Ten minutes later, as Iraqi police arrived at the scene, a suicide bomber detonated his vehicle outside the terminal, which is a main transit station

for Iraqis heading north and south. Casualties from both attacks were taken to al-Kindi hospital. At 8:45 a.m., a third car bomb was detonated at the hospital. Thirty-two Iraqi civilians and six Iraqi police are confirmed to have been killed, and at least 68 civilians were wounded in the terrorist attacks, Capt. Eeba, a civil affairs officer with 2nd Brigade, 6th Iraqi Army Division, reported. "This particular incident, where terrorists deliberately target civilians, emergency responders and hospitals, defines crimes against humanity -- period. The Iraqi people have seen once again that the terrorists have no regard for human life," said U.S. Army Col. Joseph DiSalvo, commander of 2nd Brigade Combat Team, 3rd Infantry Division (American Forces Information Service, 2005, Aug 17).

August 19 – Jordan

An al Qaeda-linked group has claimed responsibility for rocket attacks Friday that targeted but missed two U.S. military ships in the Jordanian Red Sea port of Aqaba. The three Katyusha rockets hit a warehouse and a hospital in Aqaba, killing a Jordanian soldier, and struck the nearby Israeli port city of Eilat...On Friday, three rockets were fired from a warehouse in Aqaba close to the port, a Jordanian government statement said. The warehouse had been rented a few days ago by four people of Iraqi and Egyptian descent (CNN, 2005, August 19).

August 19 – Gaza

Major attack thwarted: A 21-year-old would-be suicide bomber was detained by security forces at Gaza's Erez crossing Monday morning. Gaza resident Wafa Samir Ibrahim Bas, 21 was carrying more than 10 kilograms (more than 22 pounds) of explosives and was picked up thanks to electronic anti-terror means utilized at the crossing. Army officials

said the woman surrendered only after attempting to detonate the charge at the crossing itself. The woman was scheduled to arrive at Soroka hospital in the Southern town of Be'er Sheva for some tests Monday, and was hoping to take advantage of the medical appointment to carry out a suicide attack. During her interrogation, the would-be bomber said she was sent by the Fatah's al-Aqsa Brigades. The group sought to utilize the humanitarian permits issued to the woman and instructed her to carry out the attack at the hospital, she said (Ynetnews, 2005, August 20).

November 24 – Mahmoudiyah, Iraq

A suicide car bomber today killed 30 people outside a hospital in central Iraq, including four police guards, three women and two children. Four US soldiers who had been handing out toys to children outside the hospital in Mahmoudiya, about 30 km (20 miles) south of Baghdad, were injured in the blast. Dr. Dawoud al-Taie, the director of the Mahmoudiyah hospital, said that 35 other people were also wounded. A US military statement said: "Task Force Baghdad civil affairs soldiers were at the hospital conducting an assessment for upgrades to the facility when the car bomb detonated. Task Force Baghdad officials said the target appears to have been the hospital, but the terrorist was unable to penetrate the security perimeter before detonating (Greenburg, 2005, November 24)."

December 7 – Kirkuk, Iraq

Three hospital guards are gunned down on the job by terrorists (Hamilton Independent Media Center, 2005, December 28).

December 19 – Baghdad, Iraq

A suicidal religious extremist kills two people outside a children's hospital with a bomb

(Hamilton Independent Media Center, 2005, December 28).

References for Appendix A

- American Forces Information Service. (2005, January 20). Iraqi forces repel insurgent attack at hospital in Mosul. Retrieved September 16, 2005 from http://www.defenselink.mil/newsJan2005/n01202005_2005012001.htm
- American Forces Information Service. (2005, May 30). Iraqi aircraft crashes; operations continue throughout Iraq. Retrieved September 16, 2005 from http://www.defenselink.mil/news/May2005/20050530_1409.html
- American Forces Information Service. (2005, June 4). Iraqi ops yield suspects, weapons, missing artifacts. Retrieved September 16, 2005 from http://www.defenselink.mil/news/Jun2005/20050604_1553.html
- American Forces Information Service. (2005, July 13). Iraqi army foils three terrorist attacks. Retrieved September 16, 2005 from http://www.defenselink.mil/news/Jul2005/20050713_2047.html
- American Forces Information Service. (2005, August 17). Car bombs kill dozens near Baghdad bus station, hospital. Retrieved September 16, 2005 from http://www.defenselink.mil/news/Aug2005/20050817_2463.html
- BBC. (2005, February 12). Eighteen killed in Iraq violence. Retrieved March 2, 2006, from http://news.bbc.co.uk/1/hi/world/middle_east/4259487.stm
- CNN. (2005, February 7). Suicide bombers kill at least 27 in Iraq. Retrieved September 16, 2005, from <http://www.cnn.com/2005/WORLD/meast/02/07/iraq.main/>
- CNN. (2005, August 19). Al Qaeda claim for red sea attacks. Retrieved September 16, 2005 from <http://www.cnn.com/2005/WORLD/meast/08/19/jordan.blasts/>

DAWN. (2004, August 6). Najaf fighting claims 16 lives. Retrieved September 16, 2005 from <http://www.dawn.com/2004/08/06/top16.htm>

FOXNews. (2005, June 26). Insurgents attack across Iraq. Retrieved September 16, 2005 from <http://www.foxnews.com/story/0,2933,160712,00.html>

Greenburg, H. (2005, August 20). Female bomber nabbed. *Ynetnews*. Retrieved March 2, 2006 from <http://www.ynetnews.com/articles/0,7340,L-3101498,00.html>

Hamilton Independent Media Center. (2005, December 28). Busy year for fundamentalist terrorists. Retrieved March 2, 2006 from <http://hamilton.indymedia.org/newswire/display/183/index.php>

Ireland, M,. (2004, November 9). Car bombs kill eight, injure 60 in Iraqi violence targeted at two churches and a hospital. Retrieved November 14, 2004 from <http://www.assistnew.net/Stories/s04110036.htm>

Lutheran World Relief. (2002, June 13). Service resuming at LWR partner hospital in Liberia that was attacked and sacked last month. Retrieved September 16, 2005 from <http://www.lwr.org/news/02/061302.asp>

MacFARQUAR, N. (2002, December 31). 3 U.S. citizens slain in Yemen in rifle attack. *The New York Times*. Retrieved February 28, 2006 from <http://select.nytimes.com/gst/abstract.html?res=F50D14F63E5B0C728FDDAB0994DA404482>

National Counterterrorism Center. (2005, April 27). A chronology of significant international terrorism for 2004. Retrieved October 6, 2005 from http://www.tkb.org/documents/Downloads/NCTC_Report.pdf

- News24. (2003, December 30). Germans foil hospital attack. Retrieved October 6, 2005, from http://www.news24.com/News24/World/News/0,,2-10-1462_1464581,00.html
- PBS. (2003, August 4). Death toll in hospital bombing near Chechnya rises to 50. Retrieved September 16, 2005, from http://www.pbs.org/newshour/updates/ossetia_08-04-03.html
- The Hindu. (2005, July 3). One killed in Warangal hospital blast. Retrieved March 2, 2006, from <http://www.hindu.com/2005/07/03/stories/2005070307010100.htm>
- UN Press Release. (2003). Calm returns to Liberia's war-weary. Retrieved February 28, 2006, from <http://www.un.org/News/Press/docs/2003/afr697.doc.htm>
- U.S. Department of State. (2002, May). Patterns of global terrorism 2001. Retrieved October 11, 2005, from <http://www.state.gov/s/ct/rls/pgtrpt/2001/pdf/>
- Times Online. (2005, November 24). 30 die in bomb attack on Iraq hospital. Retrieved March 1, 2006, from <http://www.timesonline.co.uk/article/0,,7374-1889276,00.html>
- Van Marter, J. (2002, August 9). 3 killed at Presbyterian hospital in Pakistan. *PCUSA News*. Retrieved October 14, 2005 from <http://www.wfn.org/2002/08/msg00078.html>

Appendix B

Security Assessment Checklist

Hospital Access Standard:	Compliance	Planned Implementation Date	Compliance or Reassessment Date
1. All doors and entrances monitored by CCTV.	☐ Yes ☐ No ☐ N/A		
2. There is adequate security in the pharmacy to alleviate unauthorized access (Card access or keypad, locks, and CCTV).	☐ Yes ☐ No ☐ N/A		
3. All high-risk areas are monitored by CCTV.	☐ Yes ☐ No ☐ N/A		
a. Standard Operating Procedures exist for camera monitoring.	☐ Yes ☐ No ☐ N/A		
b. Recording capabilities exist with no less than 2 weeks of available media.	☐ Yes ☐ No ☐ N/A		
c. Connected to emergency power supply.	☐ Yes ☐ No ☐ N/A		
4. The hospital employs vehicle check points away from the hospital.	☐ Yes ☐ No ☐ N/A		
a. Incoming deliveries are screened away from the hospital and then allowed to proceed to the loading dock.	☐ Yes ☐ No ☐ N/A		
b. All vehicles are screened prior to entering campus. A vehicle pass is given with (A minimum of ID card and reason for visit).	☐ Yes ☐ No ☐ N/A		
c. Facility has installed barriers as needed according to the hazard vulnerability analysis.	☐ Yes ☐ No ☐ N/A		
d. Procedures exist for receiving deliveries during and after normal working hours.	☐ Yes ☐ No ☐ N/A		
5. Lab restricts access by a locking mechanism (Lock, keypad, card access, etc).	☐ Yes ☐ No ☐ N/A		
6. Facility employees / volunteers use color photo ID badges.	☐ Yes ☐ No ☐ N/A		
a. Name on the badge is large enough to be read easily including department, title, and credentials (MD, RN, etc).	☐ Yes ☐ No ☐ N/A		
b. There is an expiration date on the ID badge.	☐ Yes ☐ No ☐ N/A		
c. Procedures to follow when employees arrive without their ID.	☐ Yes ☐ No ☐ N/A		
d. Procedures for lost / stolen ID.	☐ Yes ☐ No ☐ N/A		
e. A policy exists enforcing the wear of ID's all of the time.	☐ Yes ☐ No ☐ N/A		

Hospital Access Standard: (Cont.)	Compliance	Planned Implementation Date	Compliance or Reassessment Date
7. All persons and bags entering the facility are screened.	☐ Yes ☐ No ☐ N/A		
a. Employees wear their ID badges enforced cooperatively by guards and supervisors.	☐ Yes ☐ No ☐ N/A		
b. Visitors show ID and sign-in and out and receive a visitor or out-patient badge. They are informed that the badge must be visible at all times. (Applicable for most only during non-business hours)	☐ Yes ☐ No ☐ N/A		
c. Bags and boxes are screened for contraband.	☐ Yes ☐ No ☐ N/A		
d. Policy in place for refusal of access to people who do not have positive identification or do not have a legitimate need to enter the site.	☐ Yes ☐ No ☐ N/A		
e. All contractors / vendors report to a central site to sign-in and receive distinct badges.	☐ Yes ☐ No ☐ N/A		
f. Policy that if visitors are found without a badge they will be escorted to security.	☐ Yes ☐ No ☐ N/A		
8. Mother baby unit has infant security system, which is tested daily.	☐ Yes ☐ No ☐ N/A		
a. Is the nursing station located near the entrance of the ward for constant supervision.	☐ Yes ☐ No ☐ N/A		
b. The facility is JCAHO compliant in infant security.	☐ Yes ☐ No ☐ N/A		
9. The hospital utilizes a main entrance.	☐ Yes ☐ No ☐ N/A		
10. Medical records are secured and have limited access in accordance to HIPAA standards (use of locks, keypad, or card access technologies).	☐ Yes ☐ No ☐ N/A		
11. Coordination is made with security to let them know in advance of any contractors that will be working in the facility.	☐ Yes ☐ No ☐ N/A		
12. If number of access points cannot be limited, provide security staff at each entrance.	☐ Yes ☐ No ☐ N/A		

Facilities Standard:	Compliance	Planned Implementation Date	Compliance or Reassessment Date
1. Hospital is in compliance with HAZMAT / OSHA standards for sensitive items storage.	☐ Yes ☐ No ☐ N/A		
a. All biohazard materials placed in locked freezers, incubators, and cabinets when not in use.	☐ Yes ☐ No ☐ N/A		
b. Inspect Material Safety Data Sheets (MSDS) and secure hazardous chemicals or agents in locked room, refrigerator or storage closet.	☐ Yes ☐ No ☐ N/A		
c. Oxygen storage tanks or medical gas cylinder storage areas are physically secured by fencing, locks, and CCTV.	☐ Yes ☐ No ☐ N/A		
d. Fuel tanks are physically secured by fencing, locks, and CCTV.	☐ Yes ☐ No ☐ N/A		
2. Secure Open Stem & Yoke Valve (OS&Y) secured by chain and video surveillance (CCTV) monitored 24 hours a day.	☐ Yes ☐ No ☐ N/A		
3. Video surveillance of parking areas (CCTV) monitored 24 hours a day.	☐ Yes ☐ No ☐ N/A		
4. Adequate lighting exists of concentric overlapping cones of light ensuring if one light goes out the area will still be covered.	☐ Yes ☐ No ☐ N/A		
5. Ensure storage facilities warehousing immunizations, biological agents, radiological agents, and chemical agents are physically secured by keypads, locks, and video surveillance (CCTV) monitored 24 hours a day.	☐ Yes ☐ No ☐ N/A		
6. Air intake and HVAC systems are located at least 15ft off the ground and covered by metal grates. If system is on the roof, ensure exterior ladders are secured by a locking cage.	☐ Yes ☐ No ☐ N/A		
7. There is adequate signage located in and outside the facility to direct patients where to go.	☐ Yes ☐ No ☐ N/A		
a. Signs posted at the entrance of restricted or sensitive areas indicating "Authorized Personnel Only."	☐ Yes ☐ No ☐ N/A		
b. Signs are posted at appropriate locations noting visiting hours, access requirements, trespassing, etc.	☐ Yes ☐ No ☐ N/A		

Facilities Standard: (Cont.)	Compliance	Planned Implementation Date	Compliance or Reassessment Date
8. If planning any new construction consider contracting with a Crime Prevention Through Environmental Design (CPTED) consultant or healthcare architect in the design process.	☐ Yes ☐ No ☐ N/A		
9. Hospital has fence / wall or change in landscape to differentiate from surroundings and decrease unauthorized access.	☐ Yes ☐ No ☐ N/A		
10. Hospital's power plant including generator, telephone, and water supply is physically secured by fencing, locks and video surveillance (CCTV) monitored 24 hours a day.	☐ Yes ☐ No ☐ N/A		
11. Are there any areas around the perimeter that could lead to unauthorized entry or exit?	☐ Yes ☐ No ☐ N/A		
12. Inspect all fire equipment monthly to ensure it is in working order (Extinguishers, sprinklers, and standpipes).	☐ Yes ☐ No ☐ N/A		
Information Technology Standard:	Compliance	Planned Implementation Date	Compliance or Reassessment Date
1. Create / review data disaster recovery plan (DRP) annually.	☐ Yes ☐ No ☐ N/A		
2. Ensure a secondary data source (backup) is maintained offsite or in separate complex from the original.	☐ Yes ☐ No ☐ N/A		
3. Security for LAN / WAN to include passwords, firewalls, and antivirus protection.	☐ Yes ☐ No ☐ N/A		
4. Data information center behind physical security (locks, keypad, and CCTV monitored 24 hours a day).	☐ Yes ☐ No ☐ N/A		
5. Security updates are performed regularly in accordance with hospital policy.	☐ Yes ☐ No ☐ N/A		
6. Browser controls set to detect and alert users of unauthorized access to users' machines.	☐ Yes ☐ No ☐ N/A		
7. Implement access control and encryption for sensitive information based on classification.	☐ Yes ☐ No ☐ N/A		
8. Network monitored for unauthorized access attempts.	☐ Yes ☐ No ☐ N/A		
9. Secure measures exist (VPN, SSL) for employees, volunteers, or contractors with connectivity to the network via the internet.	☐ Yes ☐ No ☐ N/A		

Information Technology Standard: (Cont.)	Compliance	Planned Implementation Date	Compliance or Reassessment Date
10. Terminated employees are removed promptly from the network.	☐ Yes ☐ No ☐ N/A		
11. Network administrator limits administrator and superuser privileges to a small number of employees.	☐ Yes ☐ No ☐ N/A		
Security Guards Standard:	Compliance	Planned Implementation Date	Compliance or Reassessment Date
1. Security services are provided on-site 24 hours a day.	☐ Yes ☐ No ☐ N/A		
a. Security is located at ED entrance.	☐ Yes ☐ No ☐ N/A		
b. There is roving security to all departments and facilities on campus.	☐ Yes ☐ No ☐ N/A		
c. Parking areas are patrolled regularly (at least hourly).	☐ Yes ☐ No ☐ N/A		
d. Security staffing is adequate to control access in the facility and safety of patients and personnel outside the facility.	☐ Yes ☐ No ☐ N/A		
e. Guards periodically check perimeter fencing and critical facilities.	☐ Yes ☐ No ☐ N/A		
2. Security Guards receive adequate training to respond to daily operational requirements. (DOD facilities must train in accordance with AR 190-56).	☐ Yes ☐ No ☐ N/A		
a. Trained and authorized to restrain visitors until local law enforcement arrives.	☐ Yes ☐ No ☐ N/A		
b. Trained in patient restraint and takedown procedures.	☐ Yes ☐ No ☐ N/A		
c. Trained in proper use of handcuffs.	☐ Yes ☐ No ☐ N/A		
d. Trained in customer service protocol and techniques.	☐ Yes ☐ No ☐ N/A		
e. Trained in key strategies to prevent or respond to workplace violence.	☐ Yes ☐ No ☐ N/A		
f. Trained in de-escalation techniques.	☐ Yes ☐ No ☐ N/A		
g. Trained in search/seizure for possible weapons.	☐ Yes ☐ No ☐ N/A		
h. Guards are BCLS certified.	☐ Yes ☐ No ☐ N/A		

Security Guards Standard: (Cont.)	Compliance	Planned Implementation Date	Compliance or Reassessment Date
i. Trained in "Lock Down" procedures for all or part of the hospital.	☐ Yes ☐ No ☐ N/A		
j. Trained in proper protocol that address handling media and VIP's.	☐ Yes ☐ No ☐ N/A		
3. Conduct a pre-employment screening including criminal background checks for all security personnel.	☐ Yes ☐ No ☐ N/A		
4. Guards have access to lists of emergency numbers for staff, facilities, and IT support available 24 hours a day.	☐ Yes ☐ No ☐ N/A		
5. Guards have access to emergency evacuation routes.	☐ Yes ☐ No ☐ N/A		
6. Guards participate in change of shift reports.	☐ Yes ☐ No ☐ N/A		
7. Conduct daily checks of security measures such as fencing, locks, CCTV, etc. to ensure proper working order.	☐ Yes ☐ No ☐ N/A		
Emergency Department Standard:	Compliance	Planned Implementation Date	Compliance or Reassessment Date
1. ED security policy to include calling security when a patient arrives with a GSW or penetrating wound.	☐ Yes ☐ No ☐ N/A		
2. Metal detector in place at entrance to assist in confiscation of weapons.	☐ Yes ☐ No ☐ N/A		
a. Policies in place and staff trained to respond to weapons brought in by patients, visitors, staff, and law enforcement.	☐ Yes ☐ No ☐ N/A		
b. Policy identifying security's response to a person's refusal to comply with use of the metal detector.	☐ Yes ☐ No ☐ N/A		
c. A "clearing barrel" used to safely clear confiscated weapons.	☐ Yes ☐ No ☐ N/A		
3. Ambulance entrance door secured with keypad, card access, or constant security.	☐ Yes ☐ No ☐ N/A		
4. Minimum standoff distance for private vehicles of 25 meters (See UFC 4-010-01).	☐ Yes ☐ No ☐ N/A		
5. ED bay doors treated with anti-shard glass film / blast resistant capabilities.	☐ Yes ☐ No ☐ N/A		
6. ED has separate restrooms and cafeteria / vending machines to reduce unauthorized persons in restricted areas.	☐ Yes ☐ No ☐ N/A		

Emergency Department Standard: (Cont.)	Compliance	Planned Implementation Date	Compliance or Reassessment Date
7. All entrances to ED monitored by CCTV.	☐ Yes ☐ No ☐ N/A		
8. A forensic policy exists for the collection of medical evidence, which includes emergency management operations.	☐ Yes ☐ No ☐ N/A		
Management Responsibilities Standard:	Compliance	Planned Implementation Date	Compliance or Reassessment Date
1. Executive Committee creates / reviews the following plans and policies annually.	☐ Yes ☐ No ☐ N/A		
a. Emergency Management Plan including disaster preparedness and pandemic policies.	☐ Yes ☐ No ☐ N/A		
b. Security Management Plan	☐ Yes ☐ No ☐ N/A		
c. Workplace Violence Policy	☐ Yes ☐ No ☐ N/A		
d. Catastrophic Emergency Evacuation Plan	☐ Yes ☐ No ☐ N/A		
e. Lockdown procedures	☐ Yes ☐ No ☐ N/A		
f. Visitor access policy	☐ Yes ☐ No ☐ N/A		
g. Plan indicating when to limit the number of facility access points.	☐ Yes ☐ No ☐ N/A		
h. Disaster Recovery Plan for hospital including provision of care off-site.	☐ Yes ☐ No ☐ N/A		
2. Agreement / MOU with local law enforcement to augment security for crowd control during emergency operations.	☐ Yes ☐ No ☐ N/A		
3. Agreement / MOU with local law enforcement to augment security during busy times (night & weekends) in ED.	☐ Yes ☐ No ☐ N/A		
4. Agreement / MOU with local fire department and HAZMAT response group to tour facility annually and identify hazards.	☐ Yes ☐ No ☐ N/A		
5. Conduct Hazard Vulnerability Analysis containing risk assessment annually.	☐ Yes ☐ No ☐ N/A		
6. Security Manager or consultant conducts annual security assessment.	☐ Yes ☐ No ☐ N/A		
7. Hold critical incident stress debriefings after incidences of violence.	☐ Yes ☐ No ☐ N/A		

Management Responsibilities Standard: (Cont.)	Compliance	Planned Implementation Date	Compliance or Reassessment Date
8. Security committee reviews issues at least quarterly to ensure identification and solution of security shortcomings.	☐ Yes ☐ No ☐ N/A		
9. In compliance with JCAHO security standards EC.2.10.	☐ Yes ☐ No ☐ N/A		
10. Management conducts terminations only when human resource representatives are present.	☐ Yes ☐ No ☐ N/A		
a. Procedure present to terminate access to voice mail, email, health information, and patient accounting systems upon termination.	☐ Yes ☐ No ☐ N/A		
b. Procedure to collect keys and ID at the time of termination.	☐ Yes ☐ No ☐ N/A		
Staff Standard:	Compliance	Planned Implementation Date	Compliance or Reassessment Date
1. Staff receives orientation / training annually of the following:	☐ Yes ☐ No ☐ N/A		
a. Emergency response plan including disaster preparedness and appropriate individual duties.	☐ Yes ☐ No ☐ N/A		
b. Security training and responsibilities for all staff.	☐ Yes ☐ No ☐ N/A		
c. Workplace violence education and response.	☐ Yes ☐ No ☐ N/A		
d. Receives training in patient DECON and PPE.	☐ Yes ☐ No ☐ N/A		
e. Protocols for employees to report suspicious activities.	☐ Yes ☐ No ☐ N/A		
f. Security codes and policies posted in all division's employee areas.	☐ Yes ☐ No ☐ N/A		
g. Emergency telephone numbers for police, fire, health, OEM and state hotlines posted prominently in areas deemed appropriate.	☐ Yes ☐ No ☐ N/A		
2. Role of security included in every employee's job description.	☐ Yes ☐ No ☐ N/A		
3. CEO emphasizes security at orientation.	☐ Yes ☐ No ☐ N/A		
4. Staff participates in annual disaster drills	☐ Yes ☐ No ☐ N/A		

Staff Standard: (Cont.)	Compliance	Planned Implementation Date	Compliance or Reassessment Date
5. Mailroom and receiving staff trained in identifying suspicious packages.	☐ Yes ☐ No ☐ N/A		
6. Conduct a pre-employment screening including criminal background checks for all personnel.	☐ Yes ☐ No ☐ N/A		
Security During Emergency Management Standard:	Compliance	Planned Implementation Date	Compliance or Reassessment Date
1. Guards have access to blueprints, maps, and utility routes.	☐ Yes ☐ No ☐ N/A		
2. Security communications are adequate and able to maintain contact with other guards and facilities Emergency Operation Center (EOC).	☐ Yes ☐ No ☐ N/A		
3. Guards participated in an emergency management exercise within the past year.	☐ Yes ☐ No ☐ N/A		
4. Security staff receives adequate emergency management training enabling a proficient response to emergencies.	☐ Yes ☐ No ☐ N/A		
a. Guards should be able to assess potential acts of terrorism by completing WMD awareness training.	☐ Yes ☐ No ☐ N/A		
b. Trained in emergency management procedures of the facility to include crowd control techniques.	☐ Yes ☐ No ☐ N/A		
c. Trained in the use of and have readily available personal protective equipment (PPE).	☐ Yes ☐ No ☐ N/A		
5. There are job action sheets for the security department outlining security staff roles in the facility's Hospital Emergency Incident Command System (HEICS).	☐ Yes ☐ No ☐ N/A		
6. All staff receive training on new threats: Avian Flu, chemical attacks, biological attacks, explosive devices (radiological, conventional), and other terrorist acts.	☐ Yes ☐ No ☐ N/A		
7. Full disaster drills held at least annually in accordance with JCAHO's standard (must hold 2 drills, one can be a tabletop exercise, but one must be a practical exercise).	☐ Yes ☐ No ☐ N/A		
8. Table top drills held at least annually.	☐ Yes ☐ No ☐ N/A		
9. Guards assume front desk duties during heightened threat levels.	☐ Yes ☐ No ☐ N/A		

Security During Emergency Management Standard: (Cont.)	Compliance	Planned Implementation Date	Compliance or Reassessment Date
10. Stand-off distances increased during heightened threat levels or emergency operations.	☐ Yes ☐ No ☐ N/A		
11. Security is at entry to parking lot with triage personnel to direct patients during emergency management procedures.	☐ Yes ☐ No ☐ N/A		
12. Emergency communications systems are up and running all of the time with the ability to communicate with security.	☐ Yes ☐ No ☐ N/A		
13. Create / maintain a plan to account for all employees during an emergency including the use of recall rosters. Conducts quarterly testing of recall rosters.	☐ Yes ☐ No ☐ N/A		
14. There is an emergency security-staffing plan that includes protocols for staff recall, employee travel, vacation and leave cancellations.	☐ Yes ☐ No ☐ N/A		

* Please note, not all items in the checklist will apply to your facility, as the hospital should consider which items are necessary to mitigate identified threats from the Hazard Vulnerability Analysis (HVA). Thus, the not applicable box was added to demonstrate acknowledgement of possible security measures a facility could utilize. This checklist should help hospital's document compliance with JCAHO's Environment of Care standards.

Assessment Conducted by: _____ Date: _____

Signature of CEO: _____ Date: _____

Signature of Hospital Board President or Representative: _____
 _____ Date: _____

References

- Arterburn, T. (2002). What hospital security should be doing now to better prepare for future activity. *Journal of Healthcare Protection Management*, 18(1), 6-14.
- Bullard, T., Strack, G., & Scharoun K. (2002). Emergency department security: A call for reassessment. *Health Care Manager*, 21(1), 65-73.
- Carroll, V. (1999). Workplace violence. *American Journal of Nursing*, 99(3), 60.
- Chen, D., Soong, S., Grimes, G., Orthner, H. (2004). Wireless local area network in a prehospital environment. *BMC Medical Informatics and Decision Making*. Retrieved February 27, 2006 from <http://www.biomedcentral.com/1472-6947/4/12>
- Grigsby, J. (n.d.). Disaster recovery plans – Now more than ever. *The Receivables Report*, 17(4), 11-12.
- Hodgson, K. (2003, March). First defense: Using design elements to strengthen security efforts. *Health Facilities Management*, 16(3), 16-20, 22, 24-25.
- Joint Commission Resources, Inc. (2005). *Hospital Accreditation Standards 2005*. U.S.A.: Author.
- Klaas, M. (2005, January). Security stat!. *Health Facilities Management*, 18(1), 22-26.
- Klein, S. (2003, May 12). Security check. *Crain's Chicago Business*, 26, 13-14.
- Leonidas, T., & O'Donnell, J. (2005, July). High tech sentinels. *Health Facilities Management*, 18(7), 25-30.
- Long, R. & Pry, W. (2002, May). Hospital security a top issue says survey. *Healthcare Benchmarks*, 9(5), 55-56.
- Luizzo, A. & Scaglione, B. (2004). How has hospital security changed since 9/11?. *Journal of Healthcare Protection Management*, 20(2), 44-48.

- McAdams, K., Russell, H., & Walukewicz, C. (2004). Gangstas – not in my hospital!. *Nursing*, 32(9), 32hn1-32hn4.
- Moss, B. (2002, July). Puzzled by security?. *Health Facilities Management*, 15(7), 17-21.
- New Jersey Hospital Association. (2005). Emergency preparedness: Hospital security 2005 update readiness assessment tool. Retrieved February 27, 2006, from www.njha.com/publications/new.publications.aspx
- Noble, S. (2002, May). As in today's world, in today's hospital, security takes many forms. *Healthcare Purchasing News*, Retrieved January 24, 2006, from <http://www.hpnonline.com/inside/2002-05/0502cover.html>
- Pietrzak, M. (2004). Threat mitigation in hospital design. *Hospital Engineering & Facilities Management*. Retrieved February 21, 2006, from <http://www.touchbriefings.com/download.cfm?fileID=1847>
- Rubin, J. (2004). Recurring pitfalls in hospital preparedness and response. *Journal of Homeland Security*. Retrieved October 4, 2005, from <http://www.homelandsecurity.org/newjournal/articles/rubin.html>
- Sarnese, P. (1997). Assessing security in the emergency department: An overview. *Journal of Emergency Nursing*, 23(1), 23-26.
- Shinkman, R. (2003). Locked down: Preserving hospital security. *Healthcare Leadership and Management Report*, 11(9), 9-13.
- Simon, H., Khan, N., & Delgado, C. (2003). Weapons detection at two urban hospitals. *Pediatric Emergency Care*, 19(4), 248-251.
- Sullivan, M., & Donnelly, B. (2005). Emergency department response to terrorism. *Topics in Emergency Medicine*, 27(1), 50-77.

Appendix C

Terrorism Mitigation Matrix

Terrorist Threat Mitigation Techniques	Product Description / Explanation	Product Website	Importance (1-5, 5=most important) *	Effectiveness Against Terrorist Attacks (1-5, 5=most effective) *	Per Unit Cost of Measure or Technique
--	-----------------------------------	-----------------	---	---	---------------------------------------

Procedural Techniques					
Visitor access control	Visitors sign-in/out of facility. Tempbadge = 1 sign-in sheet (12 badges). This will assist security and staff to enforce visitors to remain in authorized areas.	http://www.tempbadge.com/index.asp?PageAction=VIEWPROD&ProdID=202 http://securitysolutions.com/productoftheyear/2005-top20/	4	3	.59 / Sheet
ID Badges	Ensure facility utilizes photo ID's with name, Dept, credentials, and expiration date. This website sells complete ID manufacturing systems.	http://www.fargo.com/industries/more_healthcare.asp http://www.securityimaging.com/id_badge_service.html http://www.hirschelectronics.com/vm/	4	3	\$750 - \$5000 per system
Limit # of access doors to facility	Try to use a main entrance / exit. Website lists threats and ways to limit the threats. May reduce the need for security staffing.	http://www.dps.state.vt.us/homeland/dhs_bulletin.htm	4	4	Possible Reduction in \$
Facility employs security forces	Contract, in house or a combination of both.	http://www.ecamsecure.com/covered.html	5	4	Variable
Security Management Plan (Including lock-down guidelines)	Management creates / updates. Sem security is a consulting firm that can help with these services.	http://www.semsecurity.com/Hospital%20Security.htm	5	3	Variable
Emergency Management Plan (EMP)	Management creates / updates. Hospital Emergency Incident Command System (HEICS) is a main component of the response and is the standard in the industry. Includes Hazard Vulnerability Analysis (HVA) completed annually.	http://www.emsa.ca.gov/dms2/heics_main.asp www.healthcarefreeware.com/hit_ha_an.htm	5	2	Free
Facility Disaster Recovery Plan	Management creates / updates. Hospitals need to plan how to continue operations after a disaster occurs. These organizations can help.	http://www.drjil.org/ http://www.drbytamp.com/ http://www.drj.com/	NR	NR	Variable

Loading dock / Receiving protocols	Ensure trucks are screened prior to loading dock and supervised during unloading. This site describes appropriate procedures.	http://securitysolutions.com/mag/security_security_hot_spot_3/	4	4	Free
Mail room safety protocols	Ensure mail is screened and procedures in place to deal with explosive and biological threats. The USPS has a guidebook for protocols.	http://www.usps.com/communications/news/security/mailcenter.htm	4	3	Free
Stockpile immunizations / medications	Enough for initial response to disaster and for employees and family members prior to assistance from CDC's Strategic National Stockpile (SNS). The Nevada Hospital Assoc. has a model and plan to accomplish this.	http://www.nvha.net/bio/postings/prophyguide.pdf	3	2	N/A
Know how to access Strategic National Stockpile (SNS)	Ensure facility has emergency numbers to local and county health department. The health department will contact state officials (Governor must contact DHS or CDC to request SNS help).	http://www.bt.cdc.gov/stockpile/	3	2	Free
Ensure employees' families safety	Plan for provisions to vaccinate and have enough medication for employees families during emergencies. The Nevada Hospital Assoc. has a model and plan to accomplish this.	http://www.nvha.net/bio/postings/prophyguide.pdf	3	2	N/A
Participate in community collaboratives supporting Emergency Management	Ensure close relationship with local public health Dept and state epidemiological agencies. Website discusses information on collaboratives.	http://www.cacsh.org/index.html	4	3	N/A
Lobby for Legislation against violence in hospitals	CA enacted the Hospital Security Act (AB508) in 1993. The Act resulted in a reduction of violence. Website discusses current legislation.	http://www.nursingworld.org/GOVA/STATE/2003/violence1203.pdf	2	2	N/A
Training					
Terrorism Awareness	What to look for and how to spot suspected terrorist acts. Websites are online tutorials.	https://atlevel1.dtic.mil/at/ http://www.kiprc.uky.edu/trap/bioterrorism.html http://www.fema.gov/compendium/course_search.jsp?style=FE DDEPARTMENT	4	4	Free
Gang Awareness	Including local activity and history. Websites contain useful national information.	http://www.iir.com/nygc/ http://www.fastennetwork.org/Display.asp?Page=gangStats	3	2	N/A
CBRNE Training	Chemical, Biological, Radiological, Nuclear, and Explosive injuries including signs and symptoms of each. This website offers online courses with CE/CME available.	http://www.swankhealth.com/USAMRIID.html http://training.fema.gov/EMIWeb/EMICourses/EMICourse.asp http://www.osha.gov/html/faq-hazwoper.html (OSHA standards)	4	3	Free

Security Guard Competency Training	Security forces trained in all aspects of reacting to hospital related emergencies. This website (IAHSS) offers certifications within the healthcare security field.	http://www.iahss.org/cert_welcome.asp	5	4	\$110
Technology					
Metal Detectors	High crime and intercity areas. This is one of many sites offering commercial detectors.	http://www.garrett.com/security/products/pd6500i.htm	3	3	\$4,495 - \$5,495
Personal Protective Equipment (PPE)	Sufficient supplies on hand to respond to HAZMAT / CBRNE incidents. This website offers several options.	http://www.envirosafetyproducts.com/html/maxair_papr.htm http://www.tricon-env.com/index.htm	5	3	\$449
Keypads	For use in eliminating unauthorized access into restricted areas.	http://www.hirschelectronics.com/Products_ScramblePads.asp http://securitysolutions.com/productoftheyear/2005-top20/	4	3	\$400
Card Access Technologies	Similar to keypads for restricted areas including magnetic stripe and proximity card readers.	http://www.monitorsecurity.com/service.php http://securitysolutions.com/productoftheyear/2005-top20/	4	4	MS= \$328 PC= \$210
Secure ED Bay Doors	Secured by keypad, keys, or card access	http://www.hirschelectronics.com/Products_ScramblePads.asp	4	4	\$400
Manual Locksets	For any door to restrict access or theft representing the most basic security. This website offers a myriad of solutions.	http://www.secproonline.com/Stevens/SecProdPub.nsf/ProductView2?OpenForm&category=Lock	4	3	Variable
Locking Freezer / Incubator	For housing biohazard materials. The Borolabs products offer locking mechanisms.	http://www.bestlabdeals.com/Revco_General_Purpose_Laboratory_Refrigerator_p/45926.htm http://er1.org/docs/antimicrobials/Agion%20-%20Marvel%20Scientific%20Refrigeration.mht	4	3	\$3,000 - \$6,500
Community Communication System	Keeping in communication with community agencies and other hospitals during emergencies.	http://www.warningsystems.com/starter_system.htm http://www.sharpcom.com/emergency.htm	5	4	\$25,000
Detection Sensors	Senses explosives / toxic materials to be used at vehicle access points or entrances to the hospital.	http://www.sitebuys.com/explosive_detector.html	4	4	\$24,995
Iris Scan Technologies	Used to restrict access into specific areas. Recommended for high security areas.	http://www.biometricsdirect.com/Products/FA/panasonic_iris_technology.htm	2	3	\$16,917
Facial Recognition	Access into restricted areas. Product built on a DVR platform and is scaleable to fit needs.	http://www.3vr.com/	2	3	\$600 - \$2,000 / Channel
RFID Bracelets / Ankle bands	RFID is for infant abduction protection and dementia patients, also good for equipment.	http://www.securecare.com/KinderGuardID.htm	4	1	\$3.00 per Square FT

Disaster Recovery Plan for Information Technology (IT)	Plan for securing backups of electronic data at an off-site location usually through a contractor to minimized loss of data.	http://www.agilityrecovery.com/	5	3	\$200 / Month
Panic Buttons	Located at front desks, executive offices, and areas with cash functions.	http://www.mitsi.com/security/Systems/Duress%20Systems/Default.htm	4	3	\$4,375 - \$6,845
Door Alarms	Alerting unauthorized exit / entrance	http://www.sargentandgreenleaf.com/prod.php	4	4	\$136
Intrusion Alarms	Includes CCTV, passive microwave, infrared sensor, or perimeter sensor technologies. Used on or near fences and monitored by hospital security.	http://www.gviss.com/Default.aspx?tabid=82	4	4	\$5,277 - \$6,860 / Channel
Electronic Surveillance / Closed Circuit TV (CCTV)	Placed inside and outside the facility in high risk and unauthorized areas and monitored by hospital security.	http://www.gviss.com/Default.aspx?tabid=73 http://www.3vr.com/	5	4	Variable
Thermal Camera	For CCTV which registers heat patterns	http://www.cantronic.com/ir860.html http://www.thermal-eye.com/home_flash.asp	2	3	\$6,500 - \$11,350 / Camera
Day / Night Camera	Color camera by day then switching to monochrome by night to increase resolution in low light conditions.	http://www.gviss.com/Default.aspx?tabid=73	3	3	\$113 - \$2,472 / Camera
Motion Sensing Camera	Camera detects motion and follows the motion and then returns to default position.	http://www.gviss.com/Default.aspx?tabid=31	4	3	\$380 - \$2,472 / Camera
Digital Recording of CCTV	New option compared to old analog systems. Digital images are stored on hard drives and security can access any recorded moment while system is still recording. Can also be viewed on any networked computer.	http://www.3vr.com/ http://www.gviss.com/Default.aspx?tabid=61	4	3	\$581 - \$8,265 / Recorder
Mass Notification System	Provides alert warning for evacuation or shelter-in-place of everyone in or outside the facility.	http://www.madah.com http://www.whelen.com/outdoor/index.htm http://www.federalwarningsystems.com/	NR	NR	\$200K - \$300K
Design					
HVAC systems	With HEPA filter removing over 99% of biological contaminants.	http://www.pureairsystems.com/university_401.cfm	4	4	\$950 - \$2,200
Negative Pressure Capability for Lab	Safety precaution for heavy biologic testing during emergency management operations.	http://www.airwashsystems.com/	5	3	\$1,299 - \$1,999
HVAC Air Intake	Needs to be at least 15 feet off the ground with metal grate covering and opening is best angled at 45 degrees.	http://www.cdc.gov/niosh/bldvent/pdfs/2002-139.pdf (p.17)	4	3	Variable

Parking Lot Lighting	Need to have overlapping areas in case a light burns out.	http://www.residential-landscape-lighting-design.com/store/PPF/Category_ID/672/products.asp	4	4	\$630 / Light Pole
Location of Nursing Station	At a minimum the Nursery nurses station should be located by the entrance to monitor for unauthorized access.	http://www.nd.edu/~kkolberg/DesignStandards.htm (Standard 24) Located at the bottom of the page.	4	2	Depends on Design
DECON Site Location and Contaminated Water Collection	Needs to be outside away from the main facility either in temporary or permanent structure like a parking garage or DECON tent and have a system for collecting contaminated water.	http://www.osha.gov/dts/osta/bestpractices/html/hospital_firstresponders.html#appa213 http://www.tricon-env.com/index.htm (Tents)	4	3	N/A \$12,160 (Tent)
Fence, Wall, or Landscaping	The perimeter of the facility needs to be differentiated at the property line to funnel vehicles or foot traffic to appropriate entrances.	http://www.wirewall.com/ http://www.peterli.com/archive/cpm/592.shtm	4	3	\$50 - \$60 / Foot
Vehicle Check Points	Portals built for inspection of patient and cargo vehicles.	www.touchbriefings.com/download.cfm?fileID=1847&action=downloadFile (p.4)	5	5	Variable
Bollards / Barriers	Used at vehicle check points and around the facility to restrict vehicle access.	http://www.americansteelonline.com/bollard-posts.htm http://www.bigbollards.com/services_wa.htm	5	5	\$200 - \$300 / Bollard
Overpressure Outlets	Blast panels and vents that give way to blast waves from explosions decreasing damage to the building. May be engineered by using skylights that will give way to pressure from a blast.	http://www.lunor.ch/englisch/overpval.html	3	4	Depends on Design
Compartmentalization	A design where if an explosion occurred a corridor would absorb the damage and nothing beyond. To be cost effective, should occur in new construction.	http://www.utsystem.edu/fpc/docs/Rfq/uthscsa/402-236/Security_Planning_&Design_Guidelines.pdf (p.48)	4	4	Depends on design
Standoff Distance	One of the most useful blast mitigation techniques is using standoff distance of vehicles next to buildings.	www.touchbriefings.com/download.cfm?fileID=1847&action=downloadFile (p.2) http://www.fema.gov/pdf/fima/155/e155_sm.pdf (p.159)	4	4	N/A
Landscape Features	As a means for stand off distance and large boulders and mounds for blast mitigation.	http://govtsecurity.com/mag/hiding_security_plain/ http://www.asla.org/safespaces/pdf/securitydesignabstractfinal.pdf (p.15)	4	5	Variable
Heavy Concrete	Concrete is great for deflecting radiation from nuclear or dirty bombs. Most applicable for urban facilities near areas of national interest.	http://er1.org/docs/ER1_Phase_1/documents/5307.pdf	3	4	Variable
Anti Shard Blast Resistant ED Bay Doors	Ambulance bays may be at greater threat than the rest of the hospital as indicated by scenarios using ambulances as bombs.	http://www.steeldoorsdove.co.uk/Products.htm http://www.armortex.com (Call for quote) 210-661-8306 http://www.blastgard.com/home.html	4	3	Variable

Blast Resistant Film	Window covering that decreases the chance glass becomes a projectile from a blast wave.	http://www.blastgard.com/home.html http://www.madico.com/SafetyAndSecurity.htm http://www.3m.com/us/arch_construct/scpd/windowfilm/jhtml/w_i_index.jhtml	4	4	\$11 - \$14 / Square FT
Specially Treated Glass	Thicker non-shard safety glass	http://www.actionbullet.com/blast_resistant.html	4	4	\$55 - \$75 / Square FT
Blast Walls	External wall built to mitigate potential blast. Usually located next to streets and acts as barrier between building.	http://www.aigis.co.uk/buildingprotection.html http://www.gaffco.com/index.htm http://www.lifeshieldsystems.com/whatis.htm	4	4	\$35 - \$50 / Square FT
Facade Shields	Shields placed directly on the building to harden it from a blast.	http://www.lifeshieldsystems.com/whatis.htm http://www.afsindustries.com/products/blast_panels.htm	3	4	\$35 - \$50 / Square FT
Internal Wall Coverings	Usually fabricated with fiberglass or coated with KEVLAR to decrease fragments in a blast.	http://www.aigis.co.uk/blastprotectedrooms.html http://www.armortex.com/products/fiberglass.html	3	3	\$7.10 - \$46.60 / Square FT
Infection Resistant Surface Technology	Seamless non-porous surface resistant to biological and chemical contamination which is easily disinfected. Products include antimicrobial films and clear coat treatments.	http://www.agion-tech.com/HospitalProducts/default.asp http://www.microban.com/americas/products/manufacturer.html?lang=en&CategoryID=3&SubcategoryID=49&ManufacturerID=29 http://www.microbedefense.com/ppp.htm	3	3	\$.61 - \$.81 / Square FT
Self-decontaminating materials	Ionic silver metal or treatments used in air ducts, drains, and door handles which are usually havens for biological contaminants.	http://www.agion-tech.com/HospitalProducts/default.asp http://er1.org/docs/antimicrobials/Industry%20Issues%20%20AgION.mht http://er1.org/docs/antimicrobials/Sarguard.mht	3	2	Variable
Blister or Sensor Light Switches	Easily disinfected alternative to toggle switches. Regular switches have cracks and grooves making it difficult to clean and are areas that harbor potentially harmful bacteria.	http://er1.org/docs/ER1_Phase_1/Documents/5260.pdf http://www.lumitex.com/membrane_switches.html http://www.gmnameplate.com/what_we_do/membrane_switches/membraneswitches.html	3	3	\$6.24 - \$11.97 per Switch

NR = Not Rated

* Ratings were compiled from an average of responses of 8 surveyed security and emergency preparedness professionals.

Products are not paid advertisements and were chosen at random to provide a wider variety of manufacturers and distributors to choose from.

Appendix D

Resources and Websites

Medical Resources for Anti-terrorism

American Hospital Association (AHA) – Chemical and Bioterrorism Preparedness Checklist

http://www.aha.org/aha/key_issues/disaster_readiness/content/MaAtChecklistB1003.doc

American Nurses Association (ANA) – Bioterrorism and Disaster Response

<http://nursingworld.org/news/disaster/response.htm>

Association for Professionals in Infection Control and Epidemiology (APIC) – Bioterrorism Readiness Plan

<http://www.cdc.gov/ncidod/dhqp/pdf/bt/13apr99APIC-CDCBioterrorism.PDF>

Agency for Toxic Substances and Disease Registry

www.atsdr.cdc.gov

Agency for Healthcare Research and Quality (AHRQ) – Bioterrorism and Epidemic Outbreak Response Model (BERM)

<http://www.ahrq.gov/research/biomodel.htm>

Centers for Disease Control and Prevention – Biological Agent Fact Sheets

<http://www.bt.cdc.gov/agent/agentlist.asp>

Center for Disaster and Humanitarian Assistance Medicine

http://usuhs.mil/cbw/new_page_1.htm

Center for Health Affairs – Resources for Hospitals

http://www.chanet.org/emergency_preparedness_resources.htm

Chemical / Biological / Radiological Incident Handbook for first Responders

http://www.cia.gov/cia/reports/cbr_handbook/cbrbook.htm

Domestic Preparedness

<http://www.domesticpreparedness.com/>

Joint Commission Resources – Special Issue December 2001

<http://www.jcrinc.com/subscribers/perspectives.asp?durki=1122&site=10&return=1627>

National Institute of Allergy and Infectious Disease – Biodefense

<http://www3.niaid.nih.gov/biodefense/>

National Institute for Occupational Safety and Health (NIOSH) – Guidance for Filtration and Air-Cleaning Systems to Protect Building Environments from Airborne Chemical, Biological, or Radiological Attacks

<http://www.cdc.gov/niosh/docs/2003-136/2003-136.html>

National Institute for Occupational Safety and Health (NIOSH) – Pocket Guide to Chemical Hazards

<http://www.cdc.gov/niosh/npg/>

National Memorial Institute for the Prevention of Terrorism

<http://www.mipt.org/>

Terrorism and Weapons of Mass Destruction Impacting Occupational Safety and Health

<http://www1.va.gov/vasafety/page.cfm?pg=528>

The Inter Agency Board for Equipment Standardization and Inter Operability

www.iab.gov

USAF Counterproliferation Center – Terrorism Education Sources

<http://c21.maxwell.af.mil/educate.htm>

U.S. Army Medical Institute for Chemical Defense, Chemical Casualty Care Division

<https://ccc.apgea.army.mil/>

U.S. Food and Drug Administration – Counterterrorism

<http://www.fda.gov/oc/opacom/hottopics/bioterrorism.html>

U.S. General Services Administration (GSA) – Mail Center Security

www.gsa.gov/mailpolicy

U.S. General Accounting Office (GAO) – Terrorism

<http://www.gao.gov/docsearch/featured/terrorism.html>

U.S. Postal Inspection Service – Mail Center Security Guidelines

<http://www.usps.com/postalinspectors/is-pubs.htm>

WMD First Responders

<http://www.wmdfirstresponders.com/>

Security

American Institute of Architects (AIA)

<http://www.aia.org/>

American Society for Industrial Security (ASIS)

www.asisonline.org

Building Owners and Managers Association (BOMA) – Security and Emergency Preparedness

<http://www.boma.org/Advocacy/SafetyAndEmergencyPlanning/>

Central Intelligence Agency (CIA) – Chemical, Biological, Radiological Incident Handbook

http://www.cia.gov/cia/reports/cbr_handbook/cbrbook.htm

Federal Bureau of Investigation

www.fbi.gov

The Infrastructure Security Partnership

<http://www.tisp.org/tisp.cfm>

U.S. Department of Energy – National Security

<http://www.energy.gov/nationalsecurity/index.htm>

U.S. Department of Homeland Security – Ready.Gov

<http://www.ready.gov/>

Emergency Management

All-Risks-Ready Emergency Department

<http://www.erl.org/>

American Hospital Association (AHA) – Disaster Readiness

http://www.aha.org/aha/key_issues/disaster_readiness/index.html

American Red Cross

www.redcross.org

AEAS – Automated Exercise & Assessment System

www.mya eas.com

California Department of Health Services (CDHS) – Emergency Preparedness Office

<http://www.dhs.ca.gov/epo/>

California Emergency Medical Services Authority

www.emsa.ca.gov

Centers for Disease Control and Prevention (CDC) – Emergency Preparedness and Response

<http://www.bt.cdc.gov/>

Centers for Disease Control and Prevention (CDC) – Strategic National Stockpile

<http://www.bt.cdc.gov/stockpile/>

Chemical Transportation Emergency Center – Resources for Emergency Responders

<http://www.chemtrec.org/Chemtrec/Resources/>

Department of Defense (DOD) – Global Engineering Infections Surveillance and Response System

<http://www.geis.fhp.osd.mil/>

Department of Health and Human Services (DHHS) – Metropolitan Medical Response System (MMRS)

www.mmrs.hhs.gov

Disaster Help

<https://disasterhelp.gov/portal/jhtml/index.jhtml>

Environmental Protection Agency – Medical Standards

<http://www.epa.gov/epaoswer/other/medical/>

Federal Emergency Management Agency (FEMA)

<http://www.epa.gov/epaoswer/other/medical/>

HAZMAT for Healthcare

www.hazmatforhealthcare.org

Healthcare Association of Hawaii Emergency Management Program

<http://www.hah-emergency.net/default.aspx>

Healthcare Freeware – Free Healthcare Tools and Information (Including an HVA tool)

http://www.healthcarefreeware.com/hlt_ha_an.htm

HEICS – Hospital Emergency Incident Command System

<http://www.heics.com/>

International Association of Emergency Managers (IAEM)

<http://www.iaem.com/>

Joint Commission on Accreditation of Healthcare Organizations

www.jcaho.org

Joint Commission Resources – Revised Environment of Care Standards

<http://www.jcrinc.com/subscribers/perspectives.asp?durki=2515&site=10&return=1122>

Local Emergency Planning Committee (LEPC) Database

<http://yosemite.epa.gov/oswer/lepcdb.nsf/HomePage?openForm>

National Center for PTSD – Disaster mental Health Services Guidebook

<http://www.ncptsd.va.gov/publications/disaster/index.html>

National Institute for Occupational Safety and Health (NIOSH) – Emergency Response Resources

<http://www.cdc.gov/niosh/topics/emres/responders.html>

National Disaster Medical System (NDMS)

<http://ndms.dhhs.gov/index.html>

National Organization on Disability (NOD) – Emergency Preparedness Initiative

<http://www.nod.org/index.cfm?fuseaction=Page.viewPage&pageId=11>

Occupational Safety and Health Administration (OSHA) emergency preparedness tools

<http://www.osha.gov/SLTC/emergencypreparedness/index.html>

Pandemic / Avian Flu

<http://www.pandemicflu.gov/>

U.S. Army Center for Health Promotion and Preventative Medicine (USACHPPM)

<http://chppm-www.apgea.army.mil/>

Funding Opportunities for Emergency Management and Terrorism Prevention

Department of Homeland Security Office of Grants and Training

<http://www.ojp.usdoj.gov/odp/welcome.html>

Department of Homeland Security- Emergencies and Disaster Grants

<http://www.dhs.gov/dhspublic/display?theme=18>

Grants Database

<http://www.grants.gov/>

National Institute of Justice funding and training opportunities

www.ojp.usdoj.gov/nij/

Appendix E

Security Assessment and Recommendations for Landstuhl Regional Medical Center

This appendix was excluded for distribution

REPORT DOCUMENTATION PAGE					Form Approved OMB No. 0704-0188	
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.						
1. REPORT DATE (DD-MM-YYYY) 28-04-2006		2. REPORT TYPE Final Report		3. DATES COVERED (From - To) July 2005 to July 2006		
4. TITLE AND SUBTITLE Hospital Security and Force Protection: A Guide to Ensuring Patient and Employee Safety				5a. CONTRACT NUMBER		
				5b. GRANT NUMBER		
				5c. PROGRAM ELEMENT NUMBER		
				5d. PROJECT NUMBER		
6. AUTHOR(S) Blackwell, Jeffery K., CPT, MS				5e. TASK NUMBER		
				5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Landstuhl Regional Medical Center CMR 402 APO, AE 09180-0402				8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) US Army Medical Department Center and School BLDG 2841 MCCS-HFB (Army-Baylor Program in Healthcare Administration) 3151 Scott Rd, Suite 1411 Fort Sam Houston, TX 78234-6135				10. SPONSOR/MONITOR'S ACRONYM(S)		
				11. SPONSOR/MONITOR'S REPORT NUMBER(S) 28-06		
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution is unlimited						
13. SUPPLEMENTARY NOTES						
14. ABSTRACT The purpose of this study was to develop a tool to assess security measures in hospitals and provide an informational tool that would help hospitals address any shortcomings from the security assessment to deter and mitigate the effects of terrorist attacks. This study employed a qualitative approach performed using narrative meta-analysis. This was accomplished by creating a data collection sheet used to highlight salient techniques and categorize each study into three groups: hospital security, terrorism mitigation, and emergency management. The three categories of literature were used to develop the security assessment checklist, the terrorism mitigation matrix, and provide a summary of emergency management techniques. The security assessment checklist provides hospitals a tool to find vulnerabilities within their security program. Consequently, the findings are then used to mitigate any shortcomings. The terrorism mitigation matrix was created to provide administrators options for implementing terrorism and crime prevention techniques. The implementation of these tools will help hospitals prevent terrorist attacks and crime on campus.						
15. SUBJECT TERMS Hospital Security, Terrorism Mitigation, Emergency Management, Security Assessment, Hazard Vulnerability Analysis, Terrorism Time Line, Mitigation Phase, Preparedness Phase, Response Phase, Recovery Phase, Meta-Analysis, Security Audit, Security Guard						
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 136	19a. NAME OF RESPONSIBLE PERSON Education Technician	
a. REPORT U	b. ABSTRACT U	c. THIS PAGE U			19b. TELEPHONE NUMBER (Include area code) (210) 221-6443	