Journal of Hazardous Materials 115 (2004) 193–196

Journal of Hazardous Materials

www.elsevier.com/locate/jhazmat

Abstract

Force protection: today's reality

Ron Torgerson*,[1]

Versar Inc., 11990 Grant Street, Suite 500, Northglenn, CO 80233, USA

Available online 25 September 2004

Abstract

Most US infrastructure and major chemical manufacturing facilities as well as their supporting utility systems are inherently vulnerable to a terrorist attack. Force protection is a military and civilian term used to protect personnel and critical facilities and assets against would-be aggressors or terrorists. The war on terrorism is a 200–300-year war. Terrorist attacks on US soil could become as commonplace as in the State of Israel. It is very easy to penetrate infrastructure or plants as evidenced by vulnerability assessments performed for states, cities, plants, and military facilities by Versar and others around the country. Chemical, biological, radiological, nuclear, and explosive weapons can be readily used to attack facilities in the US. This paper will explain some of those vulnerabilities, outline the current DoD standard as it relates to vulnerability assessments, and explain how this may be used in commercial applications to deter potential aggressors.

Keywords: Force protection; Antiterrorism; Terrorism; Al Qaeda; Vulnerability assessment

1. Introduction

The United States of America is at war! We are thoroughly engaged in a 200–300-year war against terrorism. Our culture and way of life are at stake in this war, so it is vital we win the war! Extremist terror groups have targeted the infrastructure of the US and in particular chemical plants as an economic center. To successfully combat terrorism in our homeland, there are several things be done to protect our work force and the facilities that are integral parts of a chemical plant's mission. First, the threat must be understood. Then a defeat strategy must put in place. This strategy protects the resources of the organization. A vulnerability assessment and the subsequent mitigative measures are necessary to reduce the risk of a terrorist attack.

2. Discussion

2.1 The US is in a full press war against terrorism at home and abroad where the US has interests. The attacks on the World Trade Center in 1993 and in 2001, the attack on the Khobar Towers, the attack on the USS Cole, and the subsequent anthrax attacks, were attacks against the economic and military resources of the United States. This track record is indicative of what might happen again on US soil and abroad against US interests again. Terrorists operate in a very flexible and fluid manner where they adapt to the changing environment they live in. Terrorism is a very effective weapon as it is a relatively cheap means of waging war; terrorists are unpredictable and will change their methods to counter the protective measures the US has put in place. We see today in airport screening, electronic devices are now a concern as well as childrens' toys with potential explosives as stuffing. One of Al Qaeda's stated objectives is to attack US economic infrastructure [1]. Another stated objective of Al Qaeda is to kill four million Americans, two million of which are children [2]. As such the US chemical industry is in clear and present danger and could be in the bull's eye of the terrorist target list.

* Tel.: +1 303 452 5700x426; fax: +1 303 453 2336.
E-mail address: torgeron@versar.com.
URL: http://www.versar.com.
[1] Vice President, Federal Solutions; Fellow, Society of American Military Engineers; Risk Assessment Methodology-Water[SM], Sandia NL (SNL), Trainer; Vulnerability Assessment Methodology-Chemical Facilities[TM] SNL Trainer.

0304-3894/$ – see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.jhazmat.2004.08.016

2.2 The terrorist threat is very real in the US. Osama bin Laden still has a $25 M reward on his head from the Department of State Diplomatic Security Service. Several of his lieutenants have rewards in the multimillion-dollar range on their heads as well. Osama bin Laden's overarching strategy is to replace secular governments with Islamic Wahhabi governments. Wahhabi is a sect of Islam that is practiced in Saudi Arabia. It is based on the teachings of the Islamic "forefathers" [3]. Forefathers are defined as the first three generations of Islam, including the Prophet Muhammad. Wahhabis are also safali and believe that the Islam of today should be the same as that was practiced by the forefathers 1400 years ago [3]. That is their idea of perfect life. In that life there can be no unbelievers; Christians or Jews [4]. They also do not believe in technology, so they have no appreciation for the chemical industry's processes and believe that technology is fundamentally bad. Many of them do not read books, newspapers, or watch movies. Osama bin Laden believes Americans are the crusaders who have returned. He preaches to his followers to kill all Americans. He goes on to blame America and Israel for all the ills in the Middle East.

2.3 Aiding in bin Laden's position is the 1919 Belfour Document that basically divided the Ottoman Empire (Middle East) after World War I. So in bin Laden's mind, Israel (created after World War II) and America represent a clear and present danger to Islam as they are the focus for Christianity and Judaism. Remember, in the fundamental Moslem mindset, unbelievers are Christians and Jews and must be killed as a fundamental duty of every Moslem.

2.4 Given Al Qaeda's strong resentment to Western culture, there are several targets that fall out of their strategy to defeat the unbelievers. Recently in Manchester, England, the local police took an Al Qaeda training manual from an Al Qaeda safe house. The document is known as the "Manchester Document" and can be viewed in its entirety at http://www.usdoj.gov under "What's New." In that document the following targets are listed as avenues to overthrow Godless regimes in the West [2]:

(1) Intelligence gathering;
(2) Kidnapping enemy personnel, documents, and arms;
(3) Assassinating enemy personnel as well as tourists;
(4) Freeing captured brothers;
(5) Spreading rumors to instigate people;
(6) Blast and destroy embassies and vital economic centers;
(7) Blast places of amusement, immorality and sin—not a vital target;
(8) Blasting and destroying bridges leading in and out of cities.

2.5 Note the sixth item in the list above. Vital economic centers pertain to the economic infrastructure of the US. Chemical plants are inextricable parts of the US economy and thus are viable targets for Al Qaeda.

2.6 How do we protect ourselves against an enemy that is bent on destruction of our entire culture? It is not easy and it is expensive. An answer lies in a simple term, "force protection," that has been used by the US military for years. Force protection is used to protect personnel, families, and equipment. It applies in all situations and all locations regardless of the threat level. It is a security program providing integrated and planned applications for combating terrorist attacks against US military personnel. Force protection includes physical security, operational security, personal protective services, and intelligence and counterintelligence, plus other security programs. The overarching goal of force protection is to minimize the loss of life and the loss of critical assets. The number one priority is to keep military assets safe, but still remembering there is still some residual relative risk regardless of the force protection measures taken. Force protection is an inherent part of the facility planning and design process using the DoD Antiterrorism Force Protection (AT/FP) Construction Standards [5]. The accountability for the AT/FP program rests appropriately with the senior leadership of the respective military installations. A strong argument can be made for using the same approach, using essentially the same standards in industry.

2.7 As in commercial applications, a threat assessment must be conducted as part of the vulnerability assessment (VA) in the DoD AT/FP program. In the DoD program a VA is conducted by an outside team once every 3 years and annually by an internal team. The threat assessment is the first step in the VA process. The installation threat assessment assesses the ability of critical facilities to survive an attack. The threat assessment defines the parameters upon which the protective systems are designed to protect against. It is sometimes called the design basis threat (DBT). The protective systems will generally defeat a DBT. The DBT is based on intelligence gathering. The threat is defined by looking at an adversary's tactics, tools, explosives, and weapons that could likely be used in the attack. The definition of the DBT is based on existence, history, capability, and intentions of those wishing to do critical assets harm. The DoD has a rating system similar to the Department of Homeland Security threat level system.

2.8 The VA then is underpinned with the threat assessment. The VA addresses the susceptibility to an attack and a range of threats. The VA will drive the defensive antiterrorism measures. The VA program was created as a result of the bombing at Khobar Towers in Saudi Arabia and the bombing of the USS Cole. The VA produces a tool to assist senior leadership in their decisions on the appropriate level of AT/FP defensive measures. The VA assists the commander in protecting his/her force consisting of people and other critical assets. Governing regulations and instructions are contained in Department of Defense Instruction (DODI) 2000.16 and in DOD O-2000.12-H [5]. Both are guiding lights in the protection of DoD personnel against acts of terrorism and political turbulence.

2.9 The DoD AT/FP construction standards are mandatory for all installations at times of major renovation. They provide standards for the following: vehicular standoff distances

from facilities, the use of concrete masonry units, the use of specific glass, landscaping, and other key facility features. The standards also suggest the use of changes in land use, traffic flow, entry control, and entry control improvements that are compatible with the architectural fabric of the facility. Limiting factors for the improvements include limited resources to be allocated to the improvements, political factors, and any physical conditions that need to be considered in making the final AT/FP facility modifications.

2.10 The DoD standards are mandatory and require an AT/FP officer be appointed at each installation. The officer must formally coordinate all construction programming documents and dictate changes be made if the documents are noncompliant with the standards. The AT/FP certificate of compliance must be attached to all military construction programming documents. The core principle of the standards is defense in depth and standoff distance to protect the force – people and facilities.

2.11 So you might ask yourself what does this mean to me at a commercial facility? The answer to the question lies in the application of the mitigative measures identified in the VA. For example, in critical facilities, you should not have more than 15% of the exterior surface area covered in glass. (A critical facility is a single point of failure in the mission of the organization.) In a blast, glass is a killer of the occupants of the critical facility. Entry control to the facility is also important as are the perimeter's exterior gates. Remember, the overarching principles in this business are to inhibit unauthorized visitors and to prohibit vehicles going into or near the critical facilities. A good rule of thumb for a starting point standoff distance for a vehicle in relation to a facility is 45 m. The same is true for delivery vehicles and solid and liquid waste dumpsters and containers – all should be outside the 45 m interior perimeter. The food and water supply to the critical faculty needs to be protected and addressed in the VA as do the primary and standby power facilities and other ancillary utility systems. Communications and cyber (infostructure) networks should be protected as well as all supervisory control and data acquisition (SCADA) systems that control essential functions in a facility. Standoff distance is your best friend and normally an economical way to add force protection to your facility.

2.12 The practical application of the above steps can be taken in several forms. Glass on critical facilities should be eliminated or replaced with properly designed laminated glass or properly designed polycarbonate "glass" to withstand the design basis threat blast. Other mitigation measures can be the installation of expedient barriers such as Jersey barriers or water-filled plastic barriers (fill them with antifreeze if in northern climates). Landscaping or bollard lines can also be designed within the architectural standards of the installations. Landscaping and traffic rerouting can also be used to keep vehicles away from critical facilities.

2.13 One effective way for an adversary to enter your secure area is through your perimeter gates. Are they secure? If not, they should be designed to defeat a 15,000-pound truck loaded with explosives, traveling at 50 Mph. If the gates are not designed to this standard, they should be programmed for replacement. At gates or entry control points on your perimeter, are your entry controllers stopping and searching all trucks? If not, they should be. Do they check identification (ID) cards? If not, they should be. Do your entry controllers and all contractors (including custodial and landscaping contractors) have background investigations? If not they should. If your employees do not have background investigations, they should. At entry control points, remotely controlled barriers designed to stop 15,000-pound trucks moving at 50 Mph should be the DBT. Lastly, formal entry control procedures need to be in place along with a formal, documented training program for the entry controllers.

3. Summary

So when the above measures are implemented, do you have no risk? The answer is "no." Unless you have unlimited resources, you will always have some relative risk even after the appropriate force protection measures have been instituted. Just remember, there will be more attacks in the US and this could stretch over a 200–300 year period. Most Americans have short memories and their memories of 9/11 have already faded. Once the next attack comes, AT/FP measures will become more commonplace. The adoption of AT/FP measures in the commercial marketplace has as much utility as they do in the military sector. Is your organization ready if an aggressor comes to your perimeter ready to attack your critical assets?

Glossary

$	dollars, United States of America
AT/FP	antiterrorism/force protection
CHS–III	Certified Homeland Security, Level III
DBT	design basis threat
DoD	Department of Defense
DODI	Department of Defense Instruction
Ext.	extension
FAX	telefacsimilie
ID	identification
Inc.	incorporated
M	million
Mph	miles per hour
PE	professional engineer
RAM-W^{SM}	Risk Assessment Methodology-Water^{SM}
Ret.	retired
SCADA	supervisory control and data acquisition
SM	service mark
SNL	Sandia National Laboratories
TM	trademark
US	United States

USS United States Ship
USAF United States Air Force
VA vulnerability assessment
VAM-CF™ Vulnerability Assessment Methodology-Chemical Facilities™
WW II World War II

References

[1] D. Gold, Hatred's Kingdom, Regnery Publishing, 2003, p. 13.
[2] What's New (Al Qaeda Training Manual), http://www.doj.gov.
[3] D. Gold, Hatred's Kingdom, Regnery Publishing, 2003, pp. 18–19.
[4] D. Gold, Hatred's Kingdom, Regnery Publishing, 2003, p. 23.
[5] DoD, DODI 2000.16.