

Homeland Defense Journal *Online*

"He is best secure from dangers who is on his guard even when he seems safe." —Syrus Publilius

Homeland Defense Journal, Inc. | Suite 1003 | 4301 Wilson Boulevard | Arlington, Virginia 22203
www.homelanddefensejournal.com | Phone: 703-807-2758 | Fax: 703-807-2758

WHAT'S INSIDE

Publisher's Notes	Page 2
Letters to the Editor	Page 2
What They're Saying On The Hill	Page 6
DoD BIC Approves Five Initiatives	Page 8
DHS Reorganizes Border Security	Page 11
Shadow Bowl: A Mass Casualty Exercise	Page 12
Perseus Survey Solutions Professional Surveys Army Reserve Readiness Training Center	Page 13
At a Glance: Standing Joint Force Headquarters Homeland Security	Page 14
"Homeland Defense Funding: Waiting for the Other Shoe to Fall"	Page 15
Who's Who at the Department of Homeland Security	Page 16
FDA: New Requirement for Protecting Nation's Food Supply	Page 17
Book Review: Jane's Unconventional Weapons Response Handbook	Page 18
Firefighters Grants Online	Page 18
Calendar of Events	Page 19
Threat Report: Increase in Vulnerabilities, Decrease in Actual Attacks	Page 20
Study Shows Service Gaps in U.S. Fire Departments	Page 22
DoD Recognizes Top Info Technology Performers	Page 23
Faces In The Crowd	Page 24
Homeland Defense Business Opportunities	Page 25
Business Briefs	Page 28

OUR STAFF

PUBLISHER

Don Dickson
 ddickson@homelanddefensejournal.com
 301-455-5633

EDITOR

Marianne Dunn
 mdunn@homelanddefensejournal.com
 703-807-2495

CIRCULATION

David Dickson
 dicksond@homelanddefensejournal.com
 703-807-2758

REPORTING STAFF

George Groesbeck
 ggroesbeck@marketaccess.com
 406-782-2727

Tony Rahimi
 trahimi@homelanddefensejournal.com
 703-807-2758

EDITORIAL RESEARCH

Kim Birdsaw
 kbirdsaw@homelanddefensejournal.com

Jeff Grossman
 jgrossman@homelanddefensejournal.com

ART DIRECTOR

Dawn Woelfle
 dwoelfle@homelanddefensejournal.com
 941-746-4923

SPONSOR SALES

Cara Lombardi
 clombardi@homelanddefensejournal.com
 703-807-2743

Protecting Process Plants

Preventing terrorism attacks and sabotage

By Paul Baybutt and
 Varik Ready
 For Homeland Defense Journal

Prior to Sept. 11, 2001, threats of terrorist and criminal acts against chemical plants, oil refineries and other plants generally were not considered. However, the events of that day have mobilized many organizations to address what is now considered the real risk of the deliberate release, diversion or theft of hazardous chemicals with the intention of causing harm. Such acts could result in large numbers of public fatalities, economic and environmental

damage and loss of public confidence.

The risk of such threats must be assessed to determine

if existing security measures and safeguards are adequate or need improvement. Risk analysis approaches are rapidly being developed by both industry and government and efforts are underway to

apply and refine them. Security guidelines and security management

continued on page 3



President George Bush watches as Vice President Dick Cheney swears in Tom Ridge as the Secretary of the Department of Homeland Security in the Cross Hall Jan. 24, 2003.

Budget Request Funds War on Terror, Transformation

By Jim Garamone
 American Forces Press Service

The president's fiscal 2004 defense budget request would fund the ongoing war on terrorism while continuing the transformation of the armed forces to meet the threats of the future.

The president is asking Congress for \$379.9 billion for defense in fiscal 2004, which begins Oct. 1, 2003. That breaks down to spending \$42 million an hour, said a senior defense official who briefed reporters Friday, Jan. 31 on the 2004 request.

The budget request is \$15.3 billion more than for fiscal 2003. By service, the Army would receive \$93.7 billion, the Navy and

Marine Corps would get \$114.6 billion, and the Air Force, \$113.7 billion. Defensewide spending would be \$57.9 billion. The amount each service spends is roughly the same percentage as in the past.

Attracting and keeping quality people in the military is the highest priority of the budget. Projected military pay raises range from 2 percent to 6.25 percent. The lowest ranking service members would receive the 2 percent raise. "They are the most junior, and they don't spend a lot of time at those grades," the official said. The mid-level grades would receive the highest pay raises. As in the past, if approved, the raises go into effect Jan. 1, 2004.

continued on page 9

Special Announcement! Homeland Defense Journal is now Homeland Defense Journal Online. To continue downloading your twice-monthly issue of Homeland Defense Journal Online, go to www.homelanddefensejournal.com.

You will also be invited to subscribe to the new Homeland Defense Journal (Print Version), which will be released in Spring 2003! Subscription is free. The Homeland Defense Journal (Print Version) will bring more in-depth coverage of key topics and will continue the focus on programs, new initiatives, funding, business opportunities and information sharing among members of the homeland defense and homeland security communities.

Protecting Process Plants

continued from page 1

programs have been developed and model programs for escalating threat levels in a process plant have been described.

In security risk analyses, existing security measures and safeguards are listed, and any recommendations for improvements to reduce the likelihood and severity of terrorist and criminal acts are made for consideration by management based on the nature of the threat, process vulnerabilities, possible consequences, and existing security measures and safeguards.

Traditional security management has used the concepts of deterrence, detection and delay to protect assets. This approach worked well for the protection of assets — such as valuables in a bank vault — however, not as well when the assets are hazardous chemicals and the adversaries are terrorists. That approach would be of limited benefit in the case of hazardous materials and terrorists, as response times might not be fast enough to stop the terrorists. Also, the ability of typical response teams to neutralize a group of determined, armed and equipped terrorists is questionable. Consequently, new ways of thinking about protecting process plants are needed.

Threats

Threats might arise internally or externally. Internal threats would include sabotage and vandalism by employees, contractors or others with routine access to a facility. The main external threat is from terrorists intent on causing a large release of hazardous material, or damaging or shutting down the facility. Other threats might include the theft or diversion of chemicals, or contaminating products. Ultimately, such acts are committed

for political, religious or ideological reasons.

Possibly the most serious threat is posed by external adversaries aided by insiders. This threat would combine the knowledge of insiders with the skills and capabilities of terrorists.

Tactics and Capabilities of Adversaries

Businesses are an overwhelmingly favorite target of terrorists (see figure 1). According to "Assessing Risks from Threats to Process Plants: Threat and Vulnerability Analysis," published in the December 2002 issue of *Process Safety Progress*, threat and vulnerability analysis could be used to assess the risk of deliberate acts for a facility and identify specific threat scenarios. However, it is also possible to apply common sense to identify some of the more likely threat scenarios that might be experienced by a facility.

The release or diversion of chemicals would require breach of the process containment. This would most likely occur by manipulation of process equipment such as valves, triggering accident scenarios, or the use of explosives or projectiles.

Disgruntled employees could have detailed knowledge of a facility, its operation, layout and locations of hazardous materials. They also might have access to the facility. Manipulation of process equipment, such as valves, either directly or through the process control system, is a likely scenario. Placement of explosive devices on or adjacent to equipment is also possible. Knowledge required to build bombs and timing mechanisms is readily available, but not needed by an insider who is more likely to resort to the more direct method of process manipulation.

continued on page 4

Now, get the depth, analysis and insight you need to make your contribution to homeland security in a new print publication.

Like its bimonthly PDF sister, the monthly **Homeland Defense Journal** will be free to subscribers. Readers will receive in-depth articles and expanded coverage of homeland security funding, new initiatives, needs, requirements, products, solutions, technologies and applications that solve homeland defense and security needs as well as coverage of the people, policies and politics shaping homeland security.

NEW:

Homeland Defense Journal
Spring Release

To receive your free print publication, fill out the subscription form at

http://www.surveysolutions.com/prs/hdj/hdj_print_survey.htm

Homeland Defense Journal PDF will continue to be available online, for free, twice a month at www.homelanddefensejournal.com.

Protecting Process Plants

continued from page 3

Terrorists have strong motivations to attack, possibly even if it results in the loss of their own lives. Terrorists frequently employ bombs (see figure 2). They are not difficult to construct and could be effective even when placed some distance from the target. Terrorists also would likely possess military explosives, weapons such as automatic assault rifles and grenades, anti-personnel devices and body armor. Usually, they have trained for the attack, increasing their chances of success.

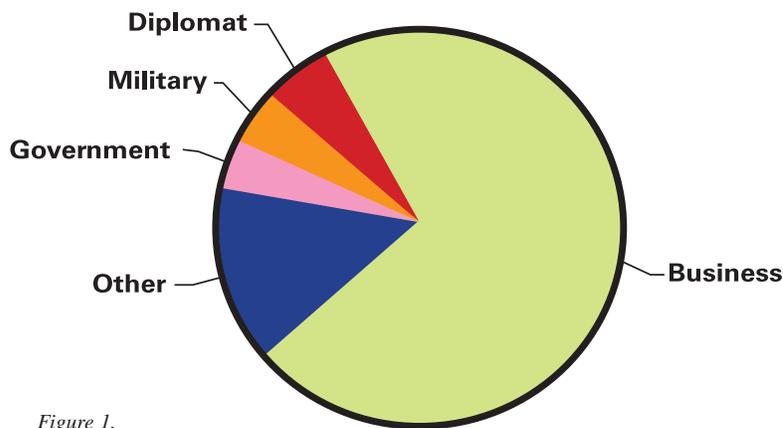


Figure 1.
Casualties in Attacks Against U.S. facilities and citizens (Data for 184 Casualties in 1999)

Source: *Patterns of Global Terrorism, U.S. Department of State Publication 10687, 1999.*

Process containment could be breached either by actions taken from outside the plant boundary or from inside. External actions include the use of bombs such as those placed in vehicles, and the use of projectiles such as rocket-propelled grenades or even aircraft. Internal actions include the placement of satchel or shaped charges.

Key Countermeasures Against Threat Scenarios

Insiders need access to critical parts of the facility to sabotage or vandalize it. Identifying and protecting critical areas would help protect against this threat, as would preventing access to critical areas by individuals who could take actions unobserved. Physical equipment, computer control systems and key support systems, such as utilities, must be protected.

Minimize the Risk of Deliberate Acts

These fairly simple steps could deter a would-be terrorist:

- What cannot be identified, cannot be attacked: Maintain a low profile
- What isn't known, cannot be used: Protect sensitive information
- Forewarned is forearmed: Monitor for suspicious activity
- Keep in control: Control vehicle bombs and the smuggling of explosive devices on site by employees, contractors or others
- Deterrence: Ensure there are visible security measures in place
- Response: Ensure intruders would be detected

Maintaining good labor relations is important. The human resources department also must monitor for employee unrest or discontent that might result in hostile actions against the facility. Background checks of new hires and screening of contractors and others who would be provided access to the facility is also important.

Terrorists would need to target a facility and obtain enough information to mount an attack. Keeping a low profile by not advertising a facility's location and the materials and quantities it handles are key protective measures. Be careful with:

- Press releases announcing new plants, expansions and new products
- Marketing information
- Company Web site
- Community outreach programs
- Public emergency response plans
- Environmental release reports
- Building plans filed with public agencies
- Information provided to vendors, contractors or consultants
- Paper trash that is not shredded
- Internet access to company computers that could be hacked
- Facility tours
- Informative signage on buildings, vessels, lines, etc.
- Technical papers
- Catalogs
- Product registries and directories
- Information provided to national and state trade associations
- Information presented at trade shows and conferences

Protecting and limiting access to sensitive information is also important, including:

- Process hazard analyses
- Process safety information
- Process security information
- RMP information
- Security vulnerability analyses
- Process descriptions
- Process drawings
- Plot plans
- Electrical classification drawings
- Emergency shutdown procedures
- Plant emergency response procedures
- Chemicals lists
- Inventories
- Formulations
- Recipes
- Client and supplier lists
- Annual reports

Information should be protected in all its forms, written, electronic and spoken.

Surveillance and information collection by terrorists are prime indicators of an incipient attack. Consequently, a counter-surveillance program to detect such activities by adversaries is critical. This would include:

continued on page 5

Protecting Process Plants

continued from page 4

- any suspicious individuals photographing the site or observing it
- contacts with employees or contractors trying to solicit information
- monitoring origins of hits on company Web site

Measures to protect against vehicle bombs would include:

- Determine danger zones on the plant exterior where vehicle bombs might be placed and monitor for the presence of vehicles in those areas.
- Restrict plant access to critical vehicles.

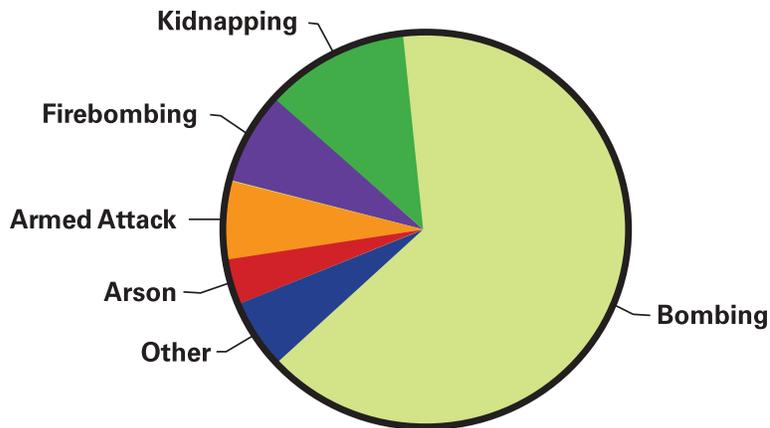


Figure 2. **Types of Attacks Against U.S. Facilities and Citizens**
 Source: *Patterns of Global Terrorism*, U.S. State Department Publication 10687, 1999.

Thoroughly search all vehicles before entry to the plant. Limit their presence in critical areas.

- Wherever possible, provide barriers to prevent vehicles being crashed into sensitive areas of the plant.
- Restrict road approaches that could be used to accelerate vehicles into plant barriers.
- Ensure you have bomb threat procedures and you know how to access a bomb disposal squad.

Packages brought on site by employees, contractors or others must also be screened for explosive devices.

While adversaries could be deterred, they might not necessarily be discouraged. However, visible security measures would likely reduce the likelihood of attack and should be employed. Note that NOT ALL security measures should be overt. Covert measures are also needed to provide an element of surprise to attackers.

Law enforcement response time and capabilities are crucial should an attack occur. Early detection of intrusion is vital for the management of such scenarios if they are not to lead to severe consequence events.

Paul Baybutt, PhD, is the president and CEO of Primatech Inc., a company specializing in process risk management.

Reserve Marine Maj. Varick Ready is the assessment team lead for Citadel LLC.



When terror strikes... How will you respond?

Your worst nightmare will become reality hours or even days before you know about it, and the two things you need to respond – time and information – are two things you probably won't have.

DynCorp's Homeland Security Incident Reporting and Tracking System (HIRTS) helps you take back the advantage. HIRTS is the first highly customizable command and control application that combines secure wireless technology, real time incident reporting and pattern recognition with infinite scalability.

Whether used on-site by first responders or in hospitals to monitor for the first signs of a WMD attack, HIRTS combines all available information to create a cohesive, real-time picture of the situation, detect trends and put time back on your side.

DynCorp
 Dynamic. Dedicated. Driven.

15000 Conference Center Drive, Chantilly, VA 20151
 887-DYN-INFO (396-4636) DSSCustomerRelations@DynCorp.com
 www.dyncorp.com