TRUCK HIJACKINGS ARE RARE, but the danger—and possible uses of the hijacked cargo—has been known for years. Terrorists slamming passenger jets into the World Trade Center and the Pentagon was a tragic reminder of just how fragile security can be. Incidents that don’t involve terrorism also provide a sense of what can occur. For example, in June 2001, a gasoline tanker crashed, turning into a high-temperature inferno that destroyed a bridge on Interstate 80 in northern New Jersey. In a 1997 incident, an overpass was melted on the New York State Thruway (Revkin B5).

A Boeing 757 jet holds nearly 11,500 gallons of fuel, while a gasoline tank trailer can carry some 9,000 gallons (Boeing; Heil Trailer). Federal officials acknowledge that a flammable liquid tanker which rams into a high-traffic bridge or building could result in substantial damage and many deaths. This article presents best practices and a checklist to help trucking companies and their employees avoid terrorist activities involving their equipment and cargo.

Shipping Freight in America

The nation’s economy was able to function following the events of Sept. 11, 2001, even with the airlines temporarily out of service. The same may not be true if the nation’s truck fleets were disabled. Consider these statistics:

On an average day, more than 17,000 containers enter U.S. ports—and only two of 100 containers are actually searched or checked by customs agents. Railroads carry more than 6 million per year, trucks more than 10 million. According to the U.S. Customs Service, more than 11.2 million trucks entered the U.S. in 2001 (Bigelow). More than 7.5 million vehicles and approximately 10.5 million holders of commercial driver’s licenses (CDLs) are widely dispersed across the U.S. Almost 2.5 million of the drivers who hold CDLs have an endorsement that allows them to transport HazMats (Clapp).

The trucking industry loses as much as $10 billion a year in cargo theft (FBI). Thieves often surprise drivers as they rest or refuel. The potential for danger is immense when one considers that stealing a load of explosives could net enough raw material for multiple bombs—or the truck itself could become a missile (Cloud).

While rental trucks seem easier to obtain than those used by carriers, commercial vehicles, buses and trucks of all types present unique security challenges. It is relatively easy to acquire a truck or bus, even on a temporary basis. Such a vehicle has a large cargo capacity and is highly mobile with easy access to key national sites and population centers (Clapp).

Overview of Needs

What might motivate a truck hijacking? Terrorists may want to:

• Cripple the ability to transport goods.
• Damage cargo to render it useless or make it hazardous to people.
• Use equipment and/or cargo to damage specific targets.

Once these potential misuses are identified, protective devices can be installed and procedures can be developed. In most cases, companies should concentrate efforts on:

1) people who have access to a truck or trailer at any time;
2) methods and equipment (e.g., equipment dispatching, preventive and emergency security methods, and equipment security);
3) facilities protection;
4) cargo and handling.
These four areas must be thoroughly evaluated for possible exposure to security-related threats. Company leadership is responsible for setting policy regarding these critical elements as well as for strategic planning.

People with Access
Those who typically come in contact with the vehicles include drivers, mechanics, washers, loading/unloading personnel and commercial vehicle inspectors. These positions must be filled by qualified employees who are provided with appropriate supervision (Van Natta and Lewis B5). Drivers, mechanics, truck washers and those loading/unloading vehicles must have had a valid U.S. driver’s license for at least three years and should not have multiple addresses. Applicants should also provide five personal references, not all of whom are immigrants or citizens of a foreign country.

An applicant’s identity should also be verified. Some carriers surpass minimum legal requirements and now fingerprint all employees and thoroughly check personal references (Wislocki 32). Combined, these measures can be very effective.

Thorough face-to-face interviews should be conducted when hiring a new driver. This helps the firm obtain information about an applicant’s personality, character, motivation, honesty, integrity and reliability. In addition, an applicant’s U.S. citizenship or immigration documents should be verified. Red flags such as gaps in employment, frequent job shifts and criminal history require further investigation.

Driver identification cards are now common. These company IDs should include the employee’s name, photo, company name and CDL information. Drivers should be prepared to present their CDL and identification cards when entering ports and shipper sites. In all cases, facilities should remain alert to suspicious behavior from drivers, applicants, shippers, consignees or the public. Drivers must also remain watchful for and report suspicious behavior witnessed on the road.

Methods & Equipment
Companies must review their security procedures to assess who has access to facilities and storage areas, as well as the adequacy of protection. Carriers should know their business partners, vendors, service providers and shippers. Security messages and training should be provided regularly to all employees. Training should be comprehensive, covering overall company security, specific procedures and the employee’s personal role in security.

Various technological innovations can improve security and communication. These include satellite tracking, surveillance systems and cell phones, as well as state-of-the-art locks and seals, alarms and engine controls (such as engine-kill switches with local and remote management). Some trucks now feature a tracking device similar to the transponders used on

On an average day, more than 17,000 containers enter U.S. ports—and only two of 100 containers are searched or checked by customs agents.
Case Studies: Tracking Vehicle & Employee Movement

Schneider National Inc., based in Green Bay, WI, had 18 truck drivers in Manhattan when the World Trade Center was attacked on Sept. 11, 2001. The company used a Qualcomm satellite system installed in its trucks to locate and send messages to each driver in order to determine his status. Each driver responded by typing in a message that he was safe. Schneider used the system to inform its 16,000 truck drivers nationwide of the events and to give instructions to those bound for metropolitan New York City or Washington, DC.


Jevic is a heavy HazMat hauler specializing in chemicals. The firm is known for conducting extensive background checks on all drivers and having one of the best safety records on the highways. Each Jevic truck is satellite-equipped, allowing it to be monitored in real-time to within 100 feet of the nearest intersection anywhere in North America.

Thirty-eight of the top 40 truckload fleets and 20 of the top 25 tank truck fleets are equipped with satellite tracking devices. The U.S. military uses a satellite system to manage logistics activities throughout Europe and to provide “situational awareness” for military operations in the Balkans. All U.S. carriers currently authorized to transport ammunition for the Dept. of Defense use a satellite system for messaging, reporting and incident response management.

Minimizing the number of interior and exterior compartments for storage in trucks, and locking those that remain with tamper-proof devices (such as seals) adds to security (Daecher). If high-tech protective devices are not available, trailer doors should be secured with a padlock. Drivers must also know to lock vehicles when stopped. Tamper-proof locking mechanisms for fifth wheels are available to protect against theft as well. Electronic engine controls, which require a code plus a key to start a vehicle, are another consideration.

Facilities Protection

Warehousing and storage facilities should be secured and monitored at all times. This requires the development and enforcement of security procedures regarding the acceptance of freight, its continued presence and its reloading for departure. Some petroleum loading terminals reportedly have begun requiring fingerprints for all drivers pulling product at those locations (Wilson).

Adequate lighting and security fencing are recommended for all facilities. Guards should be used where terminals are not populated 24 hours a day. A visitor registration process must be administered as well. Similarly, a verification process for trailer movement should be in place. Other protective measures should also be considered. These may include:

• Secure HazMat storage areas with fences or buildings.
• Require ID cards/badges for access to HazMats.
• Develop procedures that require appropriate records for removal of HazMats from secure locations.
• Protect HazMat areas via alarms and/or other security systems.
• Do not accept HazMat shipments from unfamiliar shippers.
• Ensure that locks and other protective measures are adequate.
• Train drivers to remain aware of their surroundings at all times.
• Develop standard operating procedures regarding the control of packages and train all personnel in these measures.
• Conduct security spot checks of personnel and vehicles.
• Perform credit checks and use other readily available services to determine the authenticity of a shipper’s identity.
• Be familiar with all vendors that provide services to a given facility.

Cargo & Handling

The biggest threat to the maritime industry may not be a rogue vessel ramming into a dock, but an intermodal container transporting a weapon of mass destruction into the U.S. In 2001, about 18 million of the 40-foot metal containers entered U.S. ports at about 8,000 per shipload (The Economist). Based on the known use of these containers to transport drugs, it is logical to surmise that they could be used by terrorists. In October 2001, an al Qaeda suspect commercial jets. This device transmits a truck’s location via satellite to fleet managers, while a two-way messaging system allows drivers and trucking officials to communicate. Such systems enable carriers to track loads continuously and with great accuracy. Some vehicles may feature a panic button that when pressed alerts the company’s network command center. This system can also be used to share critical information with carrier-authorized third parties, such as shippers and emergency response agencies. Truck-disabling devices that operate when someone tampers with the messaging system are currently available as well.

Marking the tops of trailers with a number-letter code for quick identification from the air or overpasses (or if the trailer is tipped over) is yet another time-tested technique. Such markings are particularly helpful if a trailer is missing and can help law enforcement in cases where finding a trailer becomes critical.

Reducing the window of opportunity for thieves and terrorists is good business practice. For example, backing a trailer next to a fixed object when parked reduces the possibility of break-ins. Some carriers are asking shippers to remain open longer in order to reduce wait time with a loaded trailer, particularly in high-crime areas (Wislocki 32).

Under no circumstances should a hitchhiker be allowed in a truck. When cargo is high value or the potential target of thieves, shadow drivers can accompany shipments. It is also best to avoid transporting HazMats near population centers and through bridges and tunnels when practical. Furthermore, the company must continually remind its drivers to strictly comply with en-route security measures.
was found inside a Canadian-bound container in an Italian port. He had enough food and water for the entire voyage to Halifax. He also had a computer, cell phone, bedding, airport plans, security passes and an aircraft mechanic’s certificate (The Economist).

To limit vulnerability, companies should screen employees and subcontractors for criminal histories and drug use; use unmarked packaging when possible; restrict cargo shipment information to only necessary personnel; limit entryways to a facility; and forbid truck drivers from interacting with warehouse staff. Some companies have invested in the latest

www.asse.org APRIL 2003 PROFESSIONAL SAFETY 24
security measures, such as real-time video camera feeds accessible to clients via the Internet and electronic tracking devices (Zalewski 14G). In extreme cases, bomb-sniffing animals can be deployed.

Armed escorts are another security measure increasingly used by logistics companies moving expensive product between distribution centers and the airport. Furthermore, developers are designing new warehouses with docks that are four to six feet high, which makes it difficult for trucks to drive through the loading doors. Architects are using landscaping (such as trees) to counter burglars who ram in front office doors and are building facilities higher than street level so that stairs and handrails for ramps become obstacles. Tilt-up construction walls are another effective security measure. Steel-reinforced concrete walls are poured at the construction site, then the nine-inch-thick slabs are tilted into place. This method, unlike hollow cinder-block walls, limits access from sledgehammer attacks. At older warehouses constructed of cinder block, vibration sensors can be used to detect attack, and motion detectors can be used to monitor passageways (Zalewski 14G).

The FBI offers the following recommendations on cargo security:

• Report cargo theft. Although some carriers are reluctant to report losses, the American Trucking Assn.’s Cargo Theft Information Processing System (Cargo TIPS) is an industrywide database to which companies can report losses. Access is limited to cargo industry members and law enforcement representatives.

• Improve background checks on drivers, dispatchers and terminal workers. Organized groups may attempt to recruit employees to learn about security weaknesses and cargo availability.

• Improve lighting and security in and around the terminal and yard.

• Enhance training in prevention and corporate security investigations.

• Increase checks of seals upon delivery.

Conclusion

Heightened security awareness is one step, but actually increasing security preparedness is another. Recent interviews conducted by Modern Bulk Transporter show that the bulk logistics sector in the U.S. remains vulnerable to terrorist attacks. Many companies have not yet implemented meaningful security plans. While expense may be a factor, the cost of doing nothing for security may be much higher than companies, society and individuals can afford.

References


The bulk logistics sector in the U.S. remains vulnerable to terrorist attacks because many firms have not yet implemented meaningful security plans.