

SECURITY NEWS



10 Tips to Help Avoid Cargo Theft

by Jerry Peck, E.J. Brooks

I. Apply for C-TPAT certification:

There's probably no better way for a company to identify its true strengths and vulnerabilities, but through a thorough self-assessment. If any company can qualify for C-TPAT status that company should immediately contact Customs and Border Protection to obtain its application. C-TPAT eligibility will require a vulnerability assessment via a Customs-supplied questionnaire. This initiative, alone, should expose most security weaknesses in that company's supply chain.

II. Ensure that the physical integrity of shipments are never compromised:

Through random container/trailer inspections, control and tracking of conveyances and their authorized drivers, both in and out of ones supply chain, will help identify irregularities. Drivers should surrender their identification to the guard, who verifies the information. The guard should record the container number, the license plate of the rig, the seal number, date and time. Random spot checks of containers are always beneficial and that they are done in the presence of another security officer.

III. Have physical access and employee/visitor controls in place:

Control of all physical accesses and who enters those accesses is paramount, if internal security procedures are to work consistently. All employees should continually have a photo identification badge. Visitors should display a clearly identifiable visitor's badge, once documentation of their identity, date and time of their visit and the person to be visited is known. Visitors should always be escorted and controlled access to sensitive areas should never be compromised.

IV. Pre-Employment Verification:

Ensure potential employees are thoroughly interviewed and screened. Have applicant submit a resume and employment history and references and have the individual sign a release form authorizing the company to perform a background check. If an individual is terminated, ensure that all company property, identification badges, passwords and other documents

are received, then escort the individual from company premises.

V. Conformance to existing regulations

With the global supply chain at risk by terrorists that will exploit any weakness, conformance to known WCO/CBT regulations will enhance safety and security for that shipper, and other shippers, who will indirectly benefit by the added diligence. Security is everyone's responsibility.

VI. Physical protection of facilities:

Ensure that perimeter fencing surrounds container and truck yards and inspect fencing regularly. Any security gates should be continually manned and that access to the terminal location should be closely monitored. External lighting, specifically in those terminal areas where little activity/traffic should be required. Video surveillance of all areas is strongly recommended. Separate logs should be kept of arriving and departing containers and trailers. Driver information, container/trailer identification, bills of lading, shipper and carrier information and seal number should be verified and any discrepancies rectified, should any exist.

VII. Training of employees is vital:

The value of trained and motivated employees is inestimable. Increasing the security awareness of all employees will enable them to respond to unexpected situations involving intruder entries, terminal incidents and minimizing the potential for theft. Annual training evaluations, at a minimum, should be provided. Preferable quarterly training sessions will be administered in areas such as security issues facing Customs and law enforcement, how to identify and report suspicious activities, recognizing internal collusion, and how to promote and maintain sound security procedures within a company's supply chain.

VIII. IT personnel are especially vulnerable to security breaches:

Ensure that the IT/data center is physically protected and set apart from all other operations.

Access should be limited to only authorized personnel and that there should be a separate source of uninterruptible power. A firewall device should be installed and all access by users is restricted to pre-determined content. Desktop access and password protection should be fully secured. A fully secured data structure should be maintained with appropriate backups at predetermined intervals.

IX. Use of high security seals:

To conform to all present and future sealing mandates and regulations the use of high security seals, as identified by ISO 17712, should become routine. Users should be trained to recognize compliant high security seals. They should be able to identify indications of the seal that would suggest theft or pilferage. To assure that the high security seals in use are in conformance, ensure that (1) test documents proving compliance to ISAO 17712 exist, (2) that the test facility is an A2LA-certified and independent test facility and that (3) the manufacturer has been audited by a certified entity.

X. Test your security program:

At little to no expense, many aspects of your security plan procedures can be tested for their viability and effectiveness. For example, you can place an unmarked vehicle in an area that's off-limits to thru traffic. Or, to assess employees' awareness of your corporate security program, with respect to authorized personnel, a person with a visitor's badge can be planted in a sensitive area of your facility. You can then monitor employee reactions to this scenario. Or, some aspect of a container's identification could be deliberately changed, such as the bill of lading, container identification, or seal sequence number. Once again, the responsiveness to gate personnel can be observed and critiqued.