Global service
built around you

North

Container Theft

Container Theft

CONTENTS

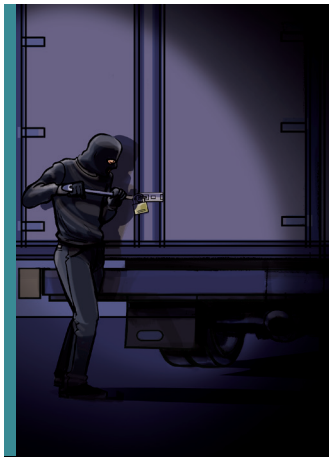
Introduction

The supply chain from supplier to consignee must remain secure to prevent the theft of cargo from the container.

Attempts to break the security of the chain by criminals may range from opportunistic or casual theft to highly developed and organised theft involving professional criminal networks.

Perpetrators may include employees or sub-contractors of the shipper, the terminal or the carrier, or could be someone external that is unrelated to any party. It is also possible that it could involve persons both on the inside and outside working in conjunction – by means of a joint operation or simply by "tipping off".

This briefing examines the links in the secure supply chain, includes points for consideration and provides loss prevention suggestions to prevent theft from containers that may be adopted by the different parties involved.



The Secure Supply Chain

The points at which a carrier's liability begins and ends depend on the type of bill of lading issued. In some cases the liability may not extend beyond the ship's rail, but if multimodal bills are in use then the carrier's liability may well extend to the point of collection at the shipper's premises up until the point of delivery at the consignee.

In the case of LCL (less than container load) shipments, the carrier may even assume responsibility for the stuffing of the container therefore increasing their liability.

This supply chain from supplier to consignee must remain secure to prevent theft of the cargo from the container. The different links of the secure supply chain and some of the potential failure points in the chain are discussed below,

complete with loss prevention suggestions which may be considered.

At Empty Release

The container as provided to the shipper must be fit for purpose and its condition must be such that it is not made vulnerable to unauthorised access to its cargo.

- Ensure the container is suitable for the intended use and is in good order.
- Scrutinise door locking arrangements and check the doors for secure riveting of fitments such as handles, locking bars and catches/hasps. Ensure there are no signs of tampering.
- When stuffing the container, locate higher value cargo towards the front wall end of the container as far away from the doors as possible.
- Use ISO 17712 compliant security bolt seals and fit them immediately upon completion of stuffing, ensuring they are properly engaged.
- Loading and holding areas to be kept secure.
- Where appropriate, use GPS tracking to monitor the movements of the container. Such systems may provide real time alarms that activate when the transit takes longer than expected.
- Consider the use of enhanced security fittings (heavy duty locks, door barriers etc.).
- The cargo description should sufficiently describe the cargo without necessarily alluding to the high potential value but care must be taken to meet customs requirements.

Container Theft (cont.)

Haulage to/from Container Terminal

Depending on geographical location there is a risk of hijacking and robbery whilst on road journeys.

Analysis carried out in the United States in 2011 by CargoNet reported that most inland cargo thefts occur at:

1. Warehouses
2. Truck stops and overnight parking areas
3. Container terminals

The report also states, rather unsurprisingly, that the most frequently stolen commodity is electronics which may point towards the thieves having prior knowledge of the contents. The report further suggests a higher probability of theft on the road over the weekend.

- Carry out vetting of subcontractors and hauliers.
- Avoid haulage being further sub-contracted to another party without prior approval.
- Keep the cargo manifest secure. Hauliers and forwarders should not be aware of the value of cargo.
- Avoid any unnecessary stops, overnight stopovers and diversions.
- Keep on main road networks and avoid secluded sections of road.
- Consider using rail transit for inland legs if the risks associated with road haulage are excessive. However, bear in mind that in some countries the risk of theft may be heightened if using the rail network.
- Check the integrity of the security seal and record seal ID number upon pickup and delivery. It may be beneficial to record the colour of the seal or even take photographs.
- Consider using escorts/convoys in high risk areas.
- Maintain increased vigilance at weekends.

At the Container Terminal

Ineffective terminal security and breaches in perimeter access control can lead not only to unauthorised persons entering the container area but also allow the flow of the stolen cargo out of the terminal.

The prominent international legislation regarding security in ports and terminals is the ISPS Code. However there are a number of accreditations relating to security management and supply chain security:

- ISO 28000:2007 Supply Chain Security Management Systems – this works on a "Plan-Do-Check-Act" model and the use of risk assessments.
- Transport Asset Protection Association (TAPA) Freight Security Requirements (FSR) – this is geared towards warehouses and logistics companies
- Custom-Trade Partnership Against Terrorism (C-TPAT) Program – this is a US program for shippers

Of the above, only the ISPS Code and ISO 28000 are recognised globally.

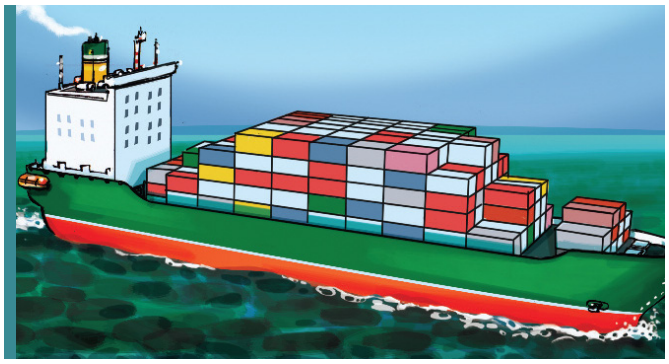
If the containers are positioned in unmonitored areas of the terminal or in stack positions allowing such easy access (such as ground level) or if the container's movements within the terminal are not properly monitored and recorded then this gives thieves the opportunity to operate undetected.

- Consider the level of confidence in the terminal's access control measures. Review the security arrangements and management and consider independent vetting by expert third parties.
- Does the terminal have ISO 28000 Supply Chain Security Management System certification?
- Review the terminal's container weighing capabilities and procedures - poorly calibrated or the improper use may lead to discrepancies not being detected.
- Consider the terminal's ability to carry out checks on the integrity and ID number of the security seal upon arrival and departure.
- Cargo information should be kept secure and ensure container movements are tracked and recorded.

Container Theft (cont.)

- Suitable planning of stack positions within the terminal for higher value cargoes, avoiding ground locations or areas with restricted CCTV coverage.
- Avoid unnecessary extended periods at the container terminals.
- Use dedicated secure inspection areas if access to the container is required (e.g. customs). Ensure any entry or inspection is documented accordingly, paying particular attention to the new security seals fitted upon re-closing.

Onboard Carrying Vessel



The carrier has an obligation to care for the cargo whilst on board the vessel, with responsibility on the crew to ensure safe carriage.

However, it is not just the ship's crew that potentially have access to a container – shore personnel and stevedores at ports of call on the way to the final discharge port may also have the opportunity.

It may be relatively easy for a crew member, stevedore or other party to break into a container, but there are notable challenges in moving the pilfered cargo on and into the shore-side black market.

- Keep the cargo manifest secure so the actual nature of the cargo is not widely known.
- Avoid stowage of valuable cargo at easily accessible positions, such as tiers 82 and 84 (bottom two tiers on deck).
- Avoid re-stows during the voyage, particular in those that require temporary landing at an intermediate port.
- Consider the possibility of stowing containers in a door-door configuration which effectively blocks access to the doors.
- Where practical and appropriate, efforts should be made to ensure security seal integrity is checked and ID number recorded upon loading and discharge from vessel.
- Maintain effective gangway security at all times when in port and remain vigilant to any unusual actions or behaviour.
- Investigate and report any noted abnormalities – such as fresh welding, paint or new rivets on the door locking arrangements.

Container Door Tampering

The container door, its locking arrangements and the security bolt seal can all be subject to tampering or attack in order to gain unauthorised access to the cargo.

Tampering may not be evident until scrutinised closely. Perpetrators can be very ingenious in their techniques and employ various methods to avoid detection.

Examples of these actions follow.

Breaking and Repairing Original Seal

Under normal circumstances, ISO 17712 compliant security bolt seals are removed by using bolt cutters and the seal is rendered unusable.

However, a neat cut that is carefully made using the appropriate power tools may allow reassembly of the seal.

Dependent on how crudely this is executed by the perpetrator, this may only be apparent when the container is delivered to the consignee and may escape cursory glances by other persons during transit.

There are also reports where seals have been subject to acid attack. The seals are most vulnerable to this kind of attack when fitted in a position where the nut or cylinder of the seal faces downwards (see Figure 1).

From reported incidents, the acid was poured into the cylinder and the corrosive action then allowed the bolt to be removed.

The result of an acid attack is that the break point would be obscured by the cylinder and therefore more difficult to detect.

Simply fitting the seal with the cylinder in the opposite position, with the nut/cylinder facing upwards, can help prevent this practice.

Fig 1: Avoid fitting seals in this orientation to prevent acid attack

Breaking and Replacing Original Seal

The distribution and custody of security seals is very difficult to control and it is extremely challenging to determine who has a particular seal at any given time and who was responsible for fitting the seal.

If new and authentic seals fall into the wrong hands, they can easily be used in the process of a crime. The original seal is broken and discarded then after the theft has taken place the replacement seal is fitted. Any discrepancy in seal identity numbers may not be noticed until much later and at that point it may be impossible to determine where the theft took place and by whom.

Container Theft (cont.)

The use of counterfeit seals is well documented, making traceability of the seal virtually impossible and pin-pointing the place and time of theft even more difficult.

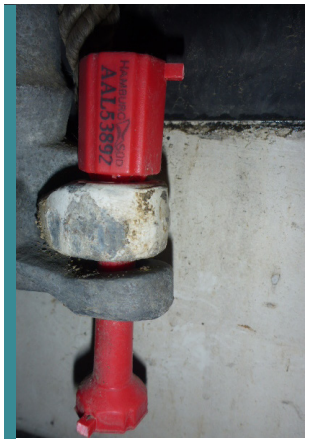


Fig 2: A counterfeit seal

Counterfeit seals are generally of low quality with identity markings poorly applied. But the counterfeit nature of a seal may be only noticeable upon close inspection with nothing untoward noticed from a cursory glance.

Taking photographs or recording the colour of the seal at the appropriate stages during transit may assist in identifying the fitting of an unauthorised replacement seal.

Pre-shipment Tampering of Seal

A security seal may have already been subjected to tampering before it has even been fitted to the container door.

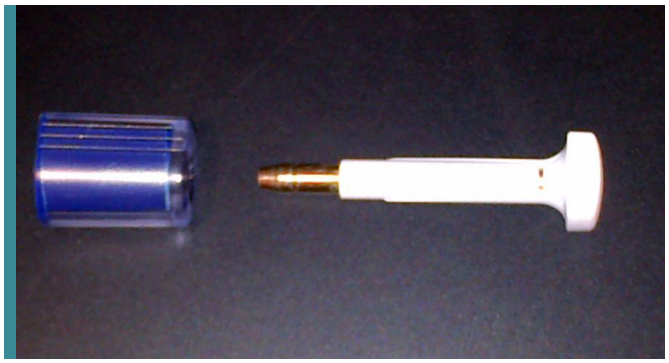


Fig 3: Parts of security bolt seal (nut or cylinder on left and a notched bolt/shaft on the right)

A known method is to attack the shaft of the bolt in way of the notch. This results in it being prevented in its ability to positively engage with the rings within the cylinder.

Another method is to insert a papier-mâché pellet into the bottom of the cylinder which prevents the bolt from going fully home

Both of these methods lead to the appearance that the two parts of the seal have been securely engaged, but in actual fact it can easily be pulled apart by hand. After the theft has taken place, the same seal can simply be re-fitted.

When checking the integrity of a seal or recording the ID number, a quick pull on the seal itself may help in identifying if it has been improperly engaged.

Tampering with the Door Handle or Locking Bars

It may be possible for the door handle to be detached from the locking bar by removing the retaining rivet as shown in Figure 4. The same principles also apply to the bolt seal catch/hasp as this too may be riveted to the container door.

After the theft has taken place, a new rivet can simply be fitted and the security seal would not have been disturbed.

It is also possible to cut the locking bars or the locking cams/cam retainers in order to open the container doors. Such an attack can be disguised by cutting behind brackets thus obscuring the cut.

The locking cams and door sill cam retainers can then be re-welded back into position after the theft has occurred.

Fig 4: Attacking the handle

Persons should remain vigilant and be suspicious of new, shiny rivets and/or the application of fresh paint in way of the locking arrangements.

Attacking the Door Retaining Plate

Container doors are generally fitted with a mechanism to prevent the left door from opening without first opening the right door.

However, this retaining plate on the overlapping door can be leveraged out of the way by the simple use of a crowbar and this can then allow access into the container though the left door.

This method of entry can be achieved without disturbing the security seal, therefore making detection more difficult. After the theft has taken place, the retaining plate can then be forced back into its original position upon re-closing.

Check for broken or disturbed coatings in way of the retaining plate and for any fresh application of paint.

Fig 5: Door retaining plate

Container Theft (cont.)

A Visible Chain

In the event of a cargo theft incident, quite often the biggest challenge is to determine the point at which the actual theft occurred. To overcome this difficulty we need supply chain visibility.

Other than a carrier having to reconsider the scope of their liability and refrain from carrying on multimodal bills of lading on troublesome routes, preventative measures are needed to protect oneself from container cargo theft at each stage of the transportation. These are described in the earlier section on the Secure Supply Chain.

In order to select the preventative measures that are appropriate to the operation and area, each link of the secure supply chain must be known and understood. The level of risk can then be assessed for each stage.

Some of these preventative actions are relatively simple and can be quite easily implemented. Others are procedural and would require significant changes and investment in security management at the various links of the secure supply chain.

An ideal system would include the verification of security seal integrity and ID numbers at each stage of the transit. However, it is very much apparent that the challenges of doing this manual checking in such a fast-paced environment, particularly during loading and discharge, are immense. Therefore its effectiveness and reliability are severely limited, bordering on impractical.

Additionally, and as described earlier, there are recorded instances where access into the container occurred without disturbing the security seal. Inspectors throughout the chain need to remain vigilant to the possibility of the tampering of the door locking arrangements.

Container weighing at various stages may highlight any discrepancies in the content, but it is important to note that there have been a number of incidents where thieves removed the cargo and replaced it with worthless material such as sand in order to give the impression the containers were still laden.

Additional measures that could be considered look towards the future and the application of new technologies, or the adaption of current technology to new uses. Such measures may include the fitting of tracking devices to the container or its cargo. It may even be appropriate for these devices to be fitted by an independent third party to ensure it can be considered impartial evidence.

There are security systems on the market that allow real time web-based tracking and have additional features such as recording the opening of a container door and sending alerts accordingly.

A further option is to fit high strength anti-tampering barriers to the container door. Or it may be appropriate to install surveillance equipment to the container.

'Intelligent' security seals or electronic seals ("e-seals") have been developed in recent years and they allow the container's location to be monitored remotely and they can alert the relevant persons when breached.

These seals do not create a more effective physical barrier to breaking into the container, but it does allow for the time and place of theft to be identified.

Limiting Your Liability

In the event of an incident it is essential that a carrier retains the ability to limit their liability under the contract of carriage.

When carrying under The Hague or Hague-Visby Rules, the package or weight limitation may apply and therefore the way the cargo quantity is described on the bill of lading can directly influence this limit.

It is equally important that any charter parties or other contracts with third parties, such as vessel sharing agreements or when using third party feeder vessels, do not expose the carrier to liabilities that exceed those under the bill of lading.

Rare & Valuable Cargo

The aforementioned arrangements and precautions may be appropriate when carrying valuable cargo in containers, but be aware that there is a distinction between "valuable" cargoes and "rare and valuable" cargoes.

This is an important distinction as it can affect P&I cover. Rare and valuable cargo must be as the name describes; both "rare" and "valuable" and does not include cargoes that are merely valuable.

Examples of rare and valuable cargo include bank notes, bullion, precious metals, works of art and sculpture.

Such cargoes must be declared to the P&I Club prior to shipment and is addressed in the Club's Rules:

North P&I Rule 19(17) LIABILITIES IN RESPECT OF CARGO

(G) RARE AND VALUABLE CARGO

"there shall be no recovery in respect of loss of or damage to specie, bullion, precious or rare metals or stones, plate, jewellery, works of art or other objects of a rare or precious nature, bank notes or other forms of currency, bonds or other negotiable instruments whether the value is declared or not unless the contract of carriage and the spaces, apparatus and means used for the carriage and the instructions given for the safe custody thereof have been approved by the Managers"

The P&I Club will need to know the exact nature of the cargo and the security arrangements for its carriage.

Container Theft (cont.)

The bill of lading should be non-negotiable (named consignee) and limited to port-to-port terms. The description of the cargo on the bill should allow the carrier to limit their liability and Hague/Hague-Visby Rules or US COGSA (as applicable) should apply.

It is also very important that an ad valorem bill of lading is not issued in such circumstances. Displaying the value of the cargo in the bill may result in the carrier losing their ability to limit liability using package or weight limitations.

In the event of voyage breakdown or an enforced transhipment there should be a contingency plan in place to ensure the cargo is never left vulnerable to theft.

Disclaimer

Published June 2015.