WHITE PAPER / CARGO SECURITY

THE VOYAGE ENDS. THE RISK DOESN'T.

Closing the Cargo-Security Gap Between the Port and the Yard

By Brett Frazee
President, DoubleLock USA | Co-Founder, STiER Security Seals

The security journey continues after discharge

For ocean cargo, reaching port can feel like the finish line. The container has crossed an ocean. It has moved through international terminals, customs processes, carrier systems and multiple layers of documentation. The doors may still carry the original high-security seal, the container number matches the bill of lading, and the shipment appears to have arrived exactly as intended. But the security journey is far from over.

In many cases, the hours and days after vessel discharge represent an entirely different risk environment. The container moves from a relatively controlled ocean transportation system into a fragmented land-side chain involving terminal operators, drayage carriers, staging areas, rail ramps, transload facilities, warehouses, drop lots and customer yards. Every one of those handoffs creates an opportunity for security to weaken. And current cargo-theft data makes the point clearly.

67%	16%	10%	~1%
TRUCKS	FACILITIES	RAIL	SEA

According to the 2025 BSI Consulting and TT Club Cargo Theft Report, trucks accounted for approximately 67% of reported U.S. cargo-theft incidents, facilities another 16%, and rail 10%. Sea-related incidents represented only about 1%. The same report identifies freight facilities, warehouses, parking areas, delivery sites and production facilities among the locations repeatedly exposed to theft. The implication for ocean freight is important:

Cargo Theft Is Becoming More Selective

This is not simply an issue of more people cutting locks in dark parking lots. Modern cargo theft increasingly combines physical attacks with intelligence, impersonation, fraudulent pickups, compromised credentials and carefully selected targets.

Verisk CargoNet estimated nearly $725 million in cargo-theft losses across the United States and Canada during 2025, a 60% increase from the prior year. Confirmed cargo theft incidents increased 18%, and the average theft value rose to approximately $274,000 as organized groups increasingly selected higher-value shipments. More recent numbers reinforce the point.

During the second quarter of 2026, CargoNet documented 677 incidents, down 26% from the same quarter in 2025. Yet estimated losses climbed to approximately $304.6 million—more than twice the prior-year level. CargoNet specifically cautioned that lower incident volume should not be interpreted as lower risk: sophisticated groups are increasingly focused on identifying the right shipment rather than simply stealing more freight. That distinction matters enormously for ocean cargo.

A container holding seafood, electronics, pharmaceuticals, copper, automotive components or other highly marketable goods may have traveled halfway around the world without incident. Once discharged, however, criminals may have access to information about the commodity, destination, carrier, pickup appointment and expected movement.

> The container is no longer an anonymous steel box at sea.
> It is inventory.

The First Mile After the Last Mile at Sea

The transition from vessel to inland transportation should therefore be treated as a security event rather than simply a logistics event. Think about what happens after discharge. A container may sit temporarily inside a marine terminal. It is released to a drayage carrier. It may travel to an off-dock yard. It might sit overnight awaiting an appointment. It may then move to a warehouse, rail ramp or distribution center before reaching the final consignee.

Responsibility can change several times while the cargo itself remains sealed. This is where small inconsistencies become important.

- Was the seal number checked against the documentation when the container left the terminal?
  - Was the seal actually inspected, or merely observed from several feet away?
  - Did the driver photograph the container doors?
  - Was there visible damage around the locking rods or hasp?
  - Was the same seal present when the container entered the destination yard?
  - Who was authorized to access the container?
  - How long did it sit unattended?
  - And perhaps most importantly: what happens when something does not match?

> If there is no defined answer to that last question, the organization does not really have a chain-of-custody process. It has a collection of records.

A Seal and a Lock Perform Different Jobs

One of the most common misunderstandings in cargo security is treating seals and locks as interchangeable. They are not. A properly selected and documented security seal provides evidence of access and supports chain-of-custody control. For applicable CTPAT-controlled movements, high-security seals meeting ISO 17712 requirements play an important role in container integrity.

CBP’s recommended seal procedures emphasize controlled seal inventories, serialized records and physical verification. They also incorporate the VVTT method—View, Verify, Twist and Tug—to confirm that the seal is correct, uncompromised and properly affixed. A physical lock serves a different purpose. Its job is resistance.

Where a seal helps answer "Has someone accessed this container?", a strong locking system addresses another question: "How difficult are we making it for someone to gain access in the first place?" For containers sitting in yards, drop lots or other land-side environments, those functions can complement each other. The seal supports identification, inspection and accountability.

The lock increases the physical effort, time, equipment and noise required for unauthorized entry. Neither replaces perimeter controls, surveillance, tracking or procedures. Cargo security works best when each layer has a defined job.

The Yard Should Be Treated as Part of the Voyage

Too often, security standards change abruptly once cargo reaches its destination region. Companies may spend significant resources qualifying carriers, documenting seals and monitoring international transit, only to place a loaded container in a poorly illuminated yard protected by an ordinary padlock and a camera nobody actively monitors. That is an inconsistent risk strategy.

The post-voyage yard should be viewed as another node in the international custody chain. Five basic disciplines can materially strengthen that environment:

Verify every arrival and departure. Container number, seal number and visible door condition should be checked at meaningful custody transfers—not simply at origin and final unloading. Photographing the doors and seal creates an inexpensive additional record.

Protect the physical entry point. Container doors are where an attacker is most likely to focus. The locking rods, hasp, lock and surrounding hardware should be evaluated as one system. For cargo that will dwell in yards or remote facilities, purpose-built container locks, shielded locking arrangements and reinforced hardware can add another physical barrier.

Control yard access. Drivers, employees, subcontractors and visitors should not move anonymously through a cargo facility. Entry, exit and authorization records create accountability and make unexplained activity easier to investigate.

Reduce unattended exposure. Lighting, cameras, fencing, container placement and dwell-time management all matter. Loaded containers should not be left in the least visible portion of a facility simply because space is available. Extended weekends and operating shutdowns deserve additional attention because unattended equipment creates time for an attack to go unnoticed.

Create an exception protocol. A damaged seal, mismatched number, disturbed locking mechanism, unexpected driver or changed pickup instruction should trigger a predefined response. Stop the movement. Verify the information independently. Document the condition. Escalate before the cargo moves deeper into the supply chain.

The objective is not to turn every distribution yard into a fortress. It is to remove unnecessary opportunities.

The Threat Is Also Moving Beyond the Fence

Physical security alone is no longer sufficient. CargoNet's first-quarter 2026 analysis describes increasingly sophisticated impersonation schemes in which criminals compromise email accounts, phone systems or industry credentials and then operate under the identity of legitimate carriers or brokers. CargoNet argues that identity verification now needs to continue throughout the shipment lifecycle rather than ending when the load is tendered. This creates a particularly dangerous combination for ocean cargo.

A criminal does not necessarily have to break into a yard if he can convince someone to release the container. That is why physical security and digital verification increasingly need to operate together. A driver arriving with the correct container number but an unexpected pickup authorization deserves scrutiny. A changed delivery location arriving by email deserves independent confirmation.

An intact seal attached to a container being released to the wrong person is not a successful security outcome. The custody chain has to protect both the container and the authority to move it.

Security Should Follow the Cargo

There is a tendency in logistics to divide transportation into separate operating worlds: ocean, terminal, drayage, rail, warehouse and final delivery. Cargo thieves do not respect those organizational boundaries. They look for the point where responsibility becomes unclear, visibility decreases or security procedures become easier to defeat.

The industry therefore needs to think about cargo security in the same way it increasingly thinks about cargo visibility: end to end.

> Know who has custody • Know what seal should be present • Know whether the doors and locking hardware have changed • Know who is authorized to move the container • Know where it is expected to go next • And create an immediate response when one of those facts does not match

The steel container itself is remarkably durable. The weakness is more often found in the systems surrounding it—the door hardware, the yard, the credentials, the records and the handoff between organizations. For ocean cargo operators, importers, freight forwarders, 3PLs and warehouse operators, that means security cannot stop when the ship reaches port.

> The voyage may be over.
> The custody chain - and the risk - are not.

About the Author

Brett Frazee

Brett Frazee is President of DoubleLock USA and Co-Founder of STiER Security Seals. DoubleLock USA provides heavy-duty physical security solutions for freight, logistics, transportation and industrial applications. STiER Security Seals focuses on tamper-evident and high-security sealing solutions supporting cargo integrity, traceability and chain-of-custody programs.

Frazee works with logistics, transportation, retail and industrial organizations on layered cargo-security strategies combining physical deterrence, tamper evidence and disciplined custody controls.

KEY TAKEAWAY

Security cannot stop when the ship reaches port. The custody chain - and the risk - continue through every land-side handoff.