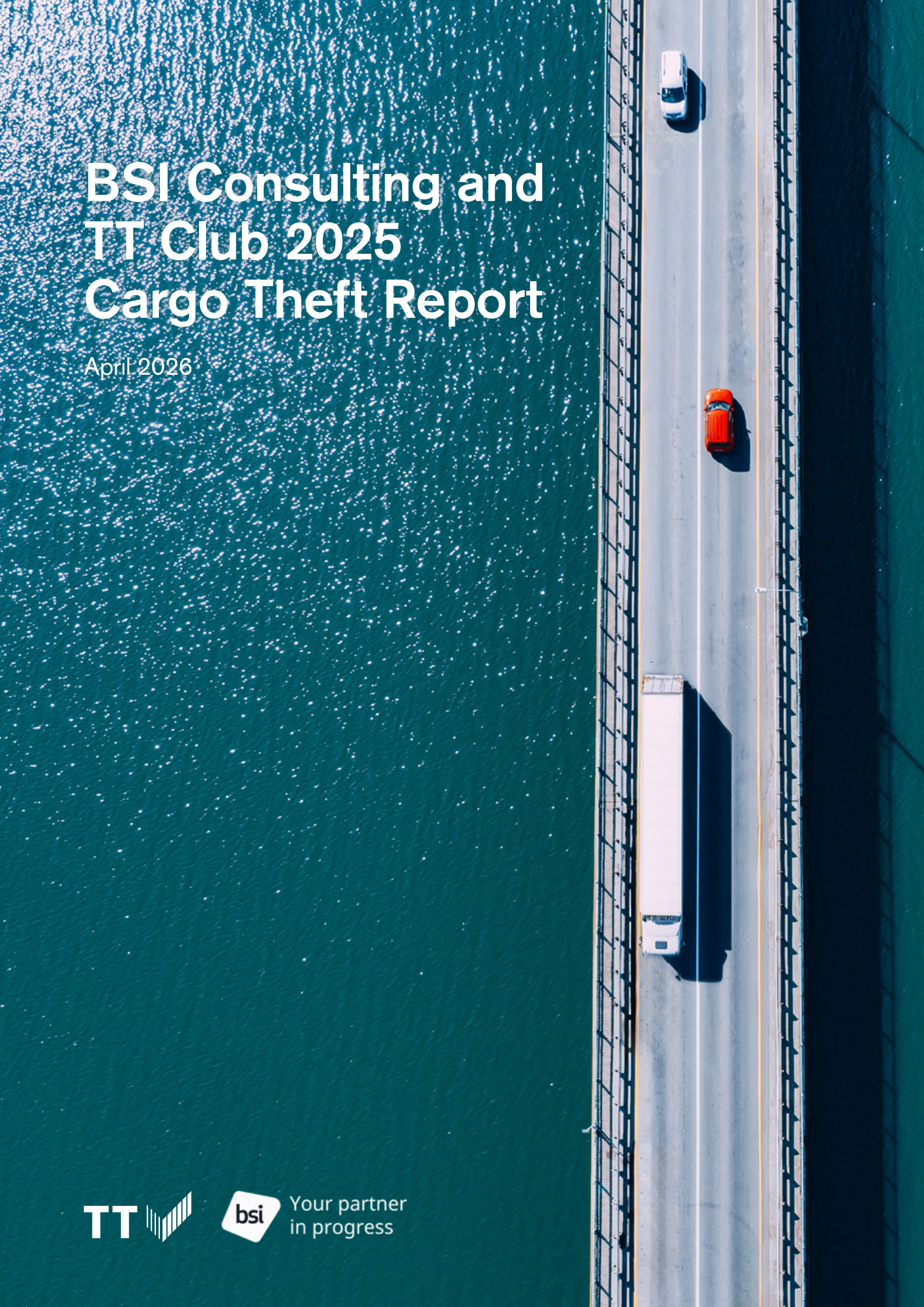
BSI Consulting and TT Club 2025 Cargo Theft Report

April 2026



TT

bsi Your partner in progress

Contents

Introduction

Cargo theft continues to present a material and evolving risk to global supply chains. Despite ongoing investment in security measures, criminal activity remains adaptive, exploiting operational complexity, market volatility and points of reduced oversight across transport modes and regions. The intelligence set out in this report confirms that cargo crime remains a persistent cause of disruption, financial loss and reputational damage.

The **BSI Consulting and TT Club 2025 Cargo Theft Report** provides a consolidated view of global cargo theft trends observed throughout 2025. Drawing on claims data, law enforcement engagement and specialist intelligence, the report examines where theft is occurring, which commodities are most exposed, and how criminal methodologies are responding to changing economic and supply chain conditions.

Consistent patterns remain evident. Food and beverage products, agricultural goods and electronics continue to dominate loss activity, reflecting their liquidity and accessibility. At the same time, the report highlights emerging areas of concern, including increased targeting of pharmaceuticals and rare earth minerals, demonstrating how rapidly criminal focus can shift in response to market value, supply constraint and regulatory pressure.

The report also reinforces the importance of understanding theft risk as a dynamic, system-wide issue. Road transport remains the most exposed modality globally, but rising rail theft, persistent facility-based losses and increasingly sophisticated multimodal schemes illustrate the need for coordinated, end-to-end risk management. Insider involvement, weak controls and fragmented responsibility continue to feature prominently in loss events.

By sharing this intelligence, TT Club and BSI Consulting seek to support informed, proactive risk management across the transport and logistics sector. Enhanced awareness of cargo theft trends, combined with intelligence-led mitigation and collaboration, remains essential to strengthening resilience and reducing exposure in an increasingly complex global trading environment.

Global cargo theft

Global cargo theft in 2025 continued to challenge supply chain resilience worldwide, with clear geographic, product-specific, and modality-driven patterns shaping the year's risk landscape.

Across major markets, Brazil, Mexico, India, the United States, Indonesia, Chile, China, Germany, and South Africa remained the top countries for recorded incidents, while Ecuador experienced one of the sharpest increases – nearly doubling its theft cases as gang-related violence intensified in coastal provinces, such as Guayas. Despite military deployments aimed at stabilising the region, escalating competition among criminal groups for control of narcotics trafficking routes is expected to sustain elevated security risks.

Food and beverage products once again led all categories of stolen goods, followed by agriculture, electronics, automotive parts, construction materials, and metals. Emerging trends included the theft of rare earth minerals from facilities in China – likely tied to their growing strategic value – and a rise in pharmaceutical thefts in India, which historically have been infrequent but now suggest elevated exposure heading into 2026 without enhanced enforcement and corporate security measures.

Trucks remained the dominant modality for cargo theft, representing roughly three-quarters of all cases. However, rail, sea, and river transport also experienced significant threats. Rail theft in the United States rose sharply between 2023 and 2025, targeting electronics, apparel, and footwear. In China, sophisticated schemes along inland waterways – particularly the Yangtze River system – involved insider collusion and organised networks targeting high-volume bulk commodities. Multimodal vulnerabilities were highlighted by a major electronics theft during sea-to-rail transfer from Guangdong to Kazakhstan, underscoring the challenges of securing cargo across varied regulatory environments and custody transfer points such as ports, rail ramps, and cross docks.

In-transit thefts continued to be the most common incident type, especially across Latin America. Armed criminal groups in Mexico continue to commit violent cargo thefts – oftentimes hijacking trucks and kidnapping drivers during thefts – and committing narcobloqueos, or road blockades, to disrupt operations through hijacking, arson, and looting. Brazil remained a major hotspot driven by organised groups using violence, document fraud, and technology to defeat GPS and facilitate high-value losses. Similar – though less frequent – patterns occurred in Ecuador and Chile. In South Africa, over half of all recorded thefts occurred in transit, with hijackings and sophisticated schemes by "blue light gangs" and insiders posing persistent risks.

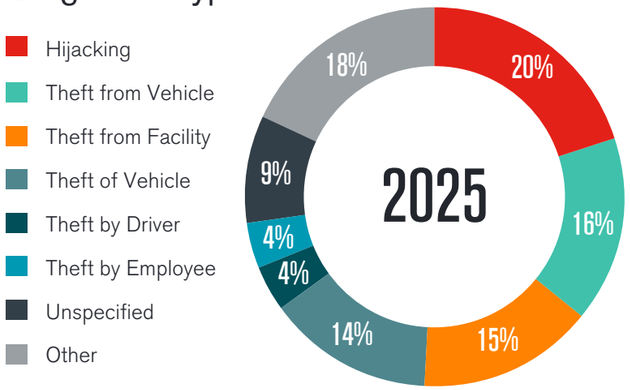
Insider involvement accounted for 22% of global cargo theft incidents, with notable concentrations in India, China, Brazil, the United States, and Indonesia. These schemes often involved incremental pilferage enabled by corrupt employees and weak inventory controls.

Link to TT Club Video Library: **Supply chain security – Fraudsters posing as authorities**

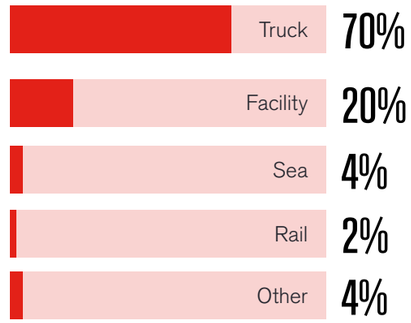
Global cargo theft trends 2025

Based on recent incident data via collaboration and partnerships with law enforcement, government, non-government, commercial partners, trade associations, open-source media reports, and input from BSI advisors and expert consultants.

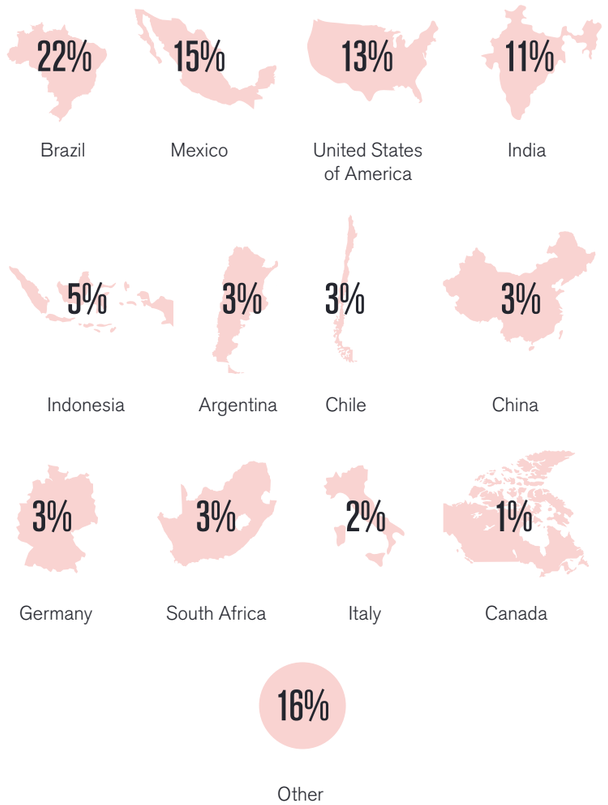
Cargo theft types



Modalities of theft



Top countries for cargo theft

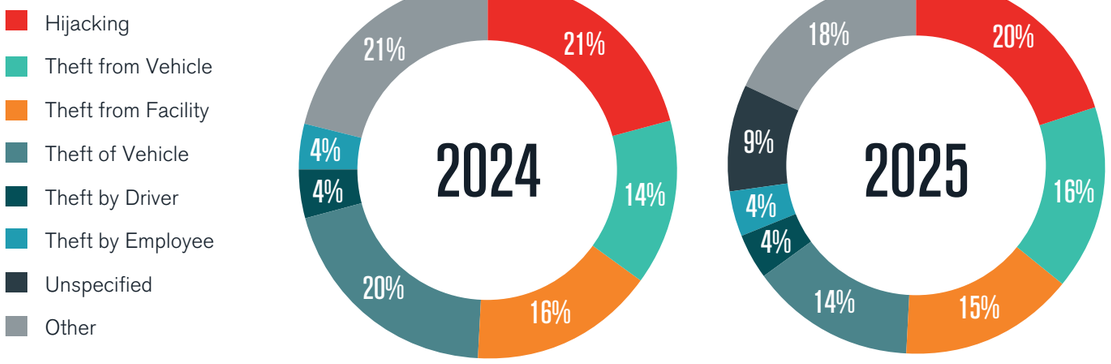


Top commodities stolen

Global cargo theft trends 2024 vs. 2025

Based on recent incident data via collaboration and partnerships with law enforcement, government, non-government, commercial partners, trade associations, open-source media reports, and input from BSI advisors and expert consultants.

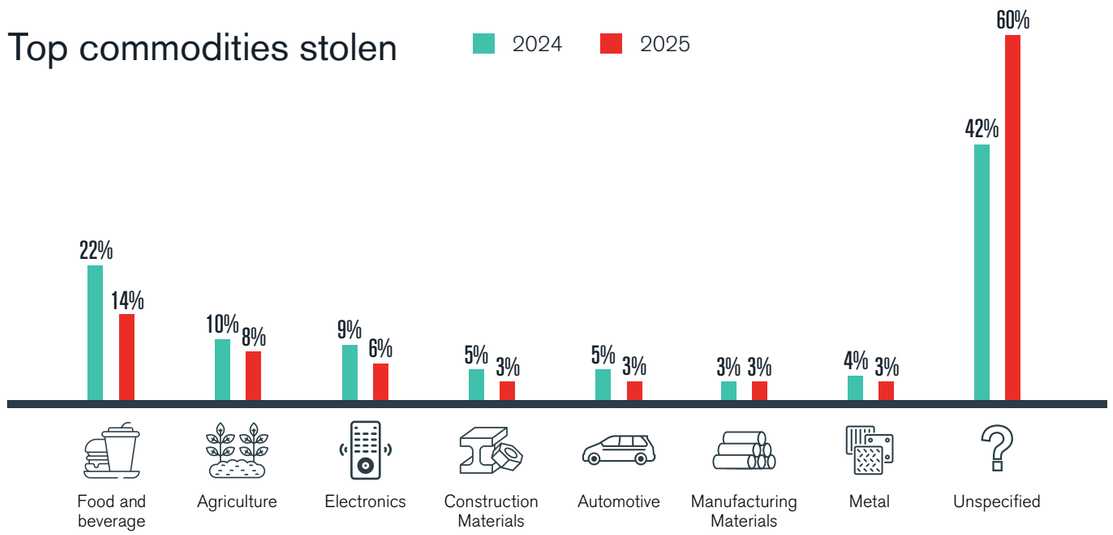
Cargo theft types



Modalities of theft

▪ Truck ▪ Facility ▪ Sea ▪ Rail ▪ Van ▪ Other ▪ Unspecified	2024	75%	18%	3%	2%	1%	1%	
	2025	70%	20%	4%	2%	1%	1%	2%

Top commodities stolen



North America

North America's 2025 cargo theft landscape was defined by continued targeting of high-value and easily monetised commodities – led by food and beverage, electronics, agriculture, automotive, pharmaceuticals, and alcohol – alongside a notable modal shift.

While trucks and facilities remained the primary theft points, rail emerged as a more targeted modality – accounting for 10% of cargo theft incidents in 2025 – compared to 2024, when it accounted for only about 6% of incidents. Hijacking remained the dominant theft type, driven heavily by persistent activity in Mexico, followed by theft of vehicle, theft from vehicle, and fictitious pickups. In-transit environments, freight and warehouse facilities, parking lots, and production sites continued to represent the most frequently targeted locations.

Spotlight on the United States

Cargo theft continues as a growing threat in the United States throughout 2025, with the country consistently ranking among the top global hotspots for supply chain crime. California (31%), Texas (15%), Illinois (7%), Florida (5%), Pennsylvania (5%), and Tennessee (5%) accounted for the highest incident volumes, while additional heightened risk states – including New Jersey, Georgia, New York, Ohio, Maryland, Arizona, and Indiana – continued to experience significant activity. Theft overwhelmingly targeted trucks (67%), followed by facilities (16%) and rail (10%), with the most frequent theft types including fictitious pickups, theft from vehicle, vehicle theft, container and trailer theft, double and triple brokering, and theft from facilities. High-risk locations included in-transit settings, freight facilities, warehouses, parking lots, delivery sites, and production facilities, reflecting widespread exposure across the supply chain. Electronics, food and beverage products, footwear, pharmaceuticals, automotive parts, and apparel were the most commonly stolen goods. Although insider involvement remained comparatively low at 6%, it doubled from the previous year, highlighting an emerging vulnerability.

Criminal activity in the United States increasingly reflects a shift from opportunistic thefts to coordinated operations led by organised theft groups and, in some cases, transnational criminal networks. Throughout 2025, law enforcement dismantled several large theft rings – including groups responsible for widespread tractor-trailer thefts and long-running diversion schemes across California. At the same time, technology-enabled strategic thefts grew more sophisticated, with criminals exploiting cybersecurity weaknesses, compromised emails, fraudulent documents, fake identities, and impersonation tactics to commit fictitious pickups, double and triple brokering, route diversions, and product hostage schemes. Recent incidents highlight these methods, including shipments redirected through fraudulent motor carrier accounts, GPS tampering, and stolen loads valued in hundreds of thousands of dollars.

Major logistics hubs such as California and Texas remained core targets, given their high freight volumes, port and border infrastructure, and the concentration of trucking activity. Criminal groups frequently exploit rest stops, freight facilities, and modal transfer points along major corridors leading from the Port of Houston and US–Mexico border crossings, where shipments are often staged with limited security.

Rail cargo theft escalated sharply in 2025, becoming one of the most critical supply chain security challenges in the United States. Organised criminal groups, including networks tied to cartels operating out of Sinaloa, Mexico, carried out highly coordinated

Modalities of Theft in the US

▪ Truck ▪ Facility ▪ Rail ▪ Van ▪ Sea	2024	78%	12%	6%	2%	1%
	2025	67%	16%	10%	3%	1%

attacks on freight trains across rural areas of Arizona and California. These operations often involved deliberate system sabotage, detailed advance planning, and armed encounters with law enforcement. Footwear – including unreleased models – electronics, appliances, and other consumer goods were among the most frequently stolen items. Clusters of incidents in major hubs such as Chicago, Memphis, and Southern California reflect the pressures created by growing cargo volumes and overstretched security resources.

Multiple factors drove the surge in activity. Elevated freight flows from West Coast ports strained rail capacity, increasing exposure as trains slowed through urban corridors or traversed long rural segments with minimal oversight. Criminal groups exploited these conditions by scouting isolated areas, cutting brake lines, damaging signal infrastructure, and using radios to coordinate offloading. Thieves routinely employed tools such as bolt cutters and saws to breach containers, while armed lookouts prevented law enforcement from intervening. Targeting patterns also suggest insider involvement, as specific high-value containers were repeatedly singled out for theft. Recent cases of rail thefts – including the damaging of rail lines – in Mexico point to a potential broadening of risk areas for rail theft as organized criminal groups are likely broadening their operations.

The expanding scale and sophistication of these operations have prompted growing calls for a unified national strategy. Rail operators and law enforcement agencies have increased countermeasures, but given the high value of targeted goods and the persistence of organised criminal groups, rail theft is expected to remain a significant threat into 2026. Additionally, industry leaders have renewed calls for legislative action, including support for the Combatting Organised Retail Crime Act (CORCA), but evolving criminal tactics, inconsistent enforcement authority, and jurisdictional complexities continue to challenge mitigation efforts. Companies should prioritise enhanced protective measures – such as GPS tracking, tamper-evident sealing systems, and strengthened coordination with federal authorities – to mitigate these rapidly evolving risks.

Europe

Cargo theft across Europe in 2025 remained a significant supply chain risk, with Germany (27%), Italy (13%), the United Kingdom (9%), France (6%), and Spain (6%) reporting the greatest number of thefts.

Theft activity was concentrated in key hotspot regions, including Hauts de France and Auvergne Rhône Alpes in France; North Rhine Westphalia, Bavaria, and Lower Saxony in Germany; Lombardy in Italy; and Nottinghamshire and Northamptonshire in the United Kingdom. Major highways such as Germany's A2 and A4, Spain's AP1 and AP7, and the UK's M1 and A1 also remained frequent targets.

While thefts primarily involved the truck modality, theft locations most often occurred at warehouses (33%), parking lots (15%), rest areas (11%), and production facilities (8%). Facility thefts saw a notable rise – particularly in Italy, Germany, Romania, and Bulgaria – reflecting an increased focus on fixed site vulnerabilities. The most common theft types included theft from facility (30%), theft from vehicle (17%), vehicle theft (15%), slash-and-grab attacks (12%), and the theft of containers or trailers (8%).

Strategic thefts, including fictitious pickups, increased in frequency as criminal groups adopted more sophisticated tactics. Examples included thieves impersonating pickup drivers to steal goods in Görlitz, Germany; criminals posing as a transport company to intercept 12,000 bottles of cognac in Charente, France; and a group in Bremen, Germany, posing as a freight forwarder to steal diverse shipments ranging from dairy and chocolate to steel and detergents.

Electronics (15%), food and beverage products (11%), and apparel (8%) were the most frequently stolen goods, with Germany reporting particularly high levels of electronics theft – such as the loss of 5,200 devices worth over USD 520,000 at Euro Rastpark in Achern. Looking ahead, we expect thieves to continue employing increasingly sophisticated methods across Europe, while common slash-and-grab incidents will persist as drivers remain exposed at unsecured parking areas and rest stops.

Spotlight on the United Kingdom

Cargo theft in the United Kingdom remains a significant and escalating threat, with losses reaching 149 million USD in 2024 and a series of high value incidents in 2025 underscoring the growing sophistication of organised criminal groups. Recent thefts – including the nine million USD smartphone heist at Heathrow, the recovery of a stolen mulled wine trailer in Rotherham, and multiple trailer break ins across South Yorkshire – reflect persistent vulnerabilities tied to trucks parked at unsecured laybys, rest areas, and transit points. A nationwide shortage of roughly 11,000 secure parking spaces continues to force drivers into high risk areas, enabling tactics such as fictitious pickups, fake license plates, and criminals posing as legitimate transport operators.

A proposed Freight Crime Bill – which aims to formally classify freight crime separately from general vehicle theft and provide law enforcement with dedicated resources and reporting mechanisms – marks an important step toward acknowledging the scale of the issue, though it remains under debate in Parliament. As infrastructure gaps persist and criminal methods evolve, cargo across the UK will likely face heightened exposure to increasingly sophisticated theft schemes in 2026.

Asia

Cargo theft, smuggling, and illicit trade dynamics across Asia continued to accelerate in 2025, with India, Indonesia, China, Bangladesh, and Vietnam emerging as the region's most affected countries.

The products most frequently targeted included agriculture, food and beverage, construction materials, manufacturing inputs, and electronics – reflecting both the region's industrial profile and the high resale value of these goods. A notable new trend was the emergence of rare earth mineral theft in China, underscoring the adaptability of thieves to pivot to high-profile items amidst product constraints such as shortages, tariffs, and export controls.

In contrast to other global hotspots where truck-related theft dominates, Asia's theft landscape is heavily facility-centric: half of all incidents occurred at warehouses and production sites, with only 36% involving trucks. The most common theft types – facility theft, theft from vehicle, and insider enabled incidents – highlight systemic vulnerabilities in storage environments and the persistent challenge of employee and contractor collusion. Insider involvement accounted for 22% of all regional thefts, with particularly high activity in India, China, and Indonesia. Many of these cases involved incremental pilferage over time, enabled by weak inventory controls and corrupt labour practices.

Complex, multimodal supply chains further intensified risk exposure. Inland waterways in China, especially the Yangtze River system, saw coordinated theft schemes involving insiders and organised criminal groups targeting bulk commodities such as coal and grain. Multimodal vulnerabilities were exemplified by a high value electronics theft during a sea to rail handoff between Guangdong and Kazakhstan – an incident that underscored how custody transfers, regulatory variations, and documentation changes generate blind spots across ports, cross docks, and rail ramps. Cyber-enabled strategic theft also rose: in China, criminals increasingly exploited online freight platforms by creating fictitious driver and company accounts to fraudulently collect cargo.

Maritime risks escalated sharply with the resurgence of sea piracy across Asian waters. Incidents rose by 85% in the first half of 2025, reaching their highest levels in nearly a decade, with the Strait of Malacca and Singapore experiencing a 281% year over year surge. While large cargo losses were rare due to strong shipboard security measures, thieves frequently stole

engine spares, ship stores, and other unsecured items. Economic hardship and inconsistent enforcement contributed to this resurgence, though targeted arrests in Indonesia helped moderate activity later in the year. Outside Southeast Asia, isolated piracy occurred near India, Bangladesh, and Vietnam, with Bangladesh notably improving port security and reducing incident volumes.

Illicit trade pressures also intensified. Counterfeiting expanded significantly due to shifting tariff structures, particularly in Vietnam, which transitioned from a transshipment hub to a centre of counterfeit production spanning apparel, pharmaceuticals, cosmetics, and personal care products. Strengthened enforcement in Vietnam has not fully kept pace with the sophistication of organised smuggling networks that leverage multi warehouse operations and cross-border routes.

Narcotics trafficking networks similarly adapted in 2025, increasingly exploiting agricultural and food shipments – cargo types subject to less rigorous inspection. A new trafficking route emerged from the United States and South America through Panama to Australia and New Zealand, where cocaine seizures surged, particularly at the Port of Tauranga. Smugglers frequently concealed drugs in duffel bags stowed inside shipping containers, exploiting complex maritime transit paths and customs vulnerabilities.

Looking ahead to 2026, the convergence of trade fraud, corruption, adaptive criminal tactics, and multimodal vulnerabilities will continue to challenge supply chain integrity across Asia and associated trade corridors. Heightened inspections, investment in advanced scanning technology, cross-agency intelligence sharing, and more uniform security standards across transport modes will be critical to reducing risk. Without coordinated action, criminals will continue to exploit regulatory gaps, insider access, and increasingly sophisticated concealment methods to target global supply chains.

Commodity driven theft risk management: Anticipating what criminals will target next

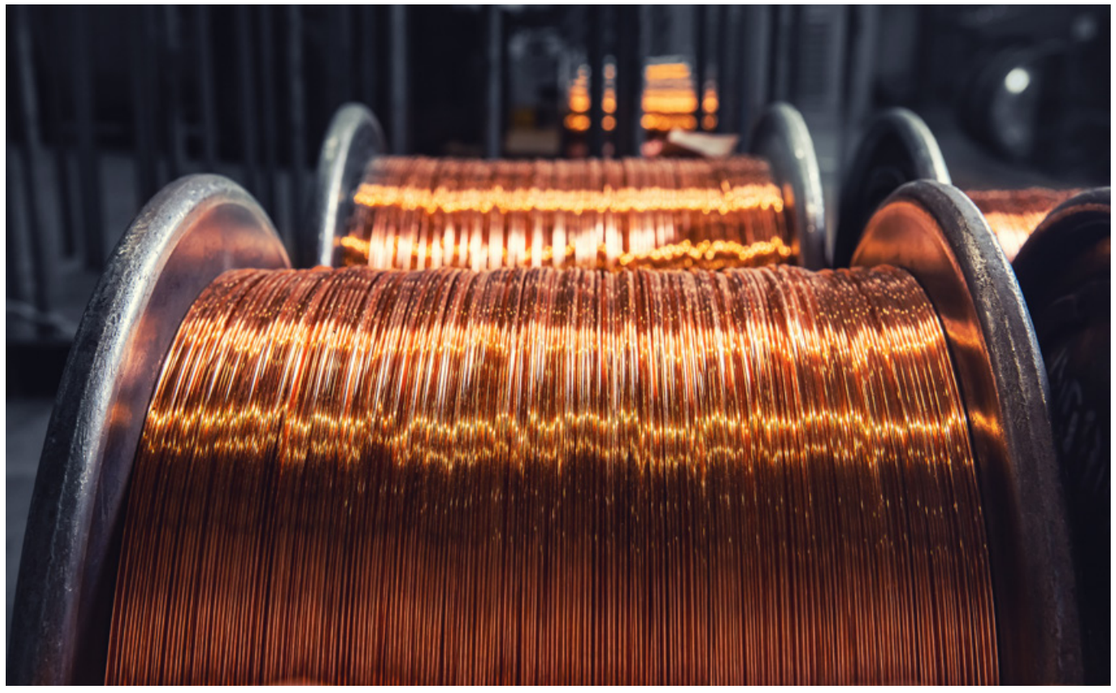
Cargo theft risk is not static. It evolves indirect response to underlying market forces, shifting supply demand dynamics, regulatory change, and commodity pricing. As highlighted throughout this year's global cargo theft intelligence, criminal groups are increasingly agile, adapting their targeting strategies to focus on goods that offer the greatest combination of value, liquidity, and ease of resale. For cargo interests, this means that historical loss experience alone is no longer sufficient to inform effective risk mitigation strategies.

Consistently targeted commodities such as food, beverages, electronics, and pharmaceuticals continue to dominate theft statistics globally. These goods benefit from stable demand, fragmented supply chains, and ready secondary markets. However, the report also identifies emerging targets – including rare earth minerals in China and a notable increase in pharmaceutical theft in India – demonstrating how rapidly criminals pivot when market conditions change. Scarcity, price volatility, and regulatory pressure can all elevate the attractiveness of goods that were previously considered lower risk.

One commodity that clearly illustrates this dynamic relationship between market forces and theft exposure is copper. Copper is a globally traded industrial metal, integral to construction, energy infrastructure, electronics, and the transition to electrification.

In recent years, average copper prices have remained at historically elevated levels, driven by sustained global demand, constrained supply, and long term structural pressures linked to decarbonisation and infrastructure investment. As the unit value of copper rises, so too does its attractiveness to organised theft groups.

TT Club's claims experience shows a clear correlation between periods of elevated copper prices and increased incident frequency. Theft is not limited to finished goods; it increasingly extends to coils, cabling, cathodes, scrap, and semi processed forms stored at yards, terminals, warehouses, and production facilities, or transported via road and rail. These losses are often opportunistic in nature but are equally enabled by weak perimeter security, insufficient oversight, and limited appreciation of how rapidly a commodity's risk profile can change.



This relationship between market value and theft risk underlines the importance of commodity specific risk assessment. Cargo interests should actively monitor market indicators – such as sustained price increases, supply shortages, or regulatory shifts – that may signal heightened exposure. Goods that were previously treated as routine cargo may warrant enhanced controls when market conditions change. Failure to reassess risk in light of these external drivers can result in security measures lagging behind the threat.

Effective commodity driven theft risk management requires dynamic, rather than static, mitigation strategies. Security controls should be adjusted according to the value, liquidity, and attractiveness of the cargo at a given point in time. For higher risk commodities such as copper, this may include enhanced physical security at storage locations, tighter access control, improved inventory reconciliation, and increased scrutiny of subcontracted transport providers. During transit, routing, parking practices, and dwell times should be reviewed to minimise exposure, particularly in known theft hotspots or unsecured staging areas.

Enhanced oversight is also critical for commodities that are becoming newly attractive. The report highlights how criminals are increasingly targeting goods influenced by geopolitical tension, export controls, or supply constraints. Early warning indicators drawn from claims trends, intelligence reporting, and market analysis should be used to identify these shifts before losses escalate. Collaboration between commercial, operational, and risk management teams is essential to ensure that emerging threats are recognised and addressed promptly.

Ultimately, anticipating what thieves will target next is as important as understanding what they targeted last year. By aligning loss prevention strategies with underlying market forces, cargo interests can better protect themselves against evolving theft patterns. Proactive monitoring of commodity markets – combined with flexible, intelligence led risk mitigation – will be essential in reducing exposure in an environment where criminal behaviour is increasingly driven by economic opportunity.

Load Boards and the changing risk environment in modern freight brokerage

Introduction

Load boards have become a defining feature of contemporary road freight brokerage. Their widespread use reflects the industry's continued drive for efficiency, market visibility, and flexible capacity. However, the same features that make these platforms attractive also introduce meaningful operational, security, and liability risks. The increasing sophistication of criminal activity, particularly through the use of data scraping, artificial intelligence, and impersonation techniques, has magnified these concerns. This article examines how load boards function, why they have become so prevalent, and what measures organisations can take to mitigate the exposures that accompany their use.

The role of Load Boards in freight operations

Load boards, often referred to as freight exchange platforms, are digital marketplaces designed to match available shipments with available motor carriers. They originally emerged after deregulation in the 1980s, functioning as simple bulletin boards intended to reduce empty running miles and accelerate subcontracting. Today they form an integral part of the North American trucking ecosystem. An estimated 75–80% of shipments are now directed toward load boards, not only as a last resort but as a routine method of securing capacity.

In practice, load boards support operational efficiency by providing immediate access to a national carrier pool. They offer visibility into prevailing capacity and rates, and they allow brokers to resolve urgent capacity shortages when a planned carrier falls through. Their convenience has made them ubiquitous, yet it has also normalised their use in circumstances for which they may not be appropriate.

Internal and Public Load Boards: Different risk profiles

A central distinction lies between private, internal load boards and public platforms. Large logistics operators have developed proprietary systems that admit only vetted and pre approved carriers. These closed environments allow for tighter administrative control, closer monitoring, and the application of established management processes. The restricted participant pool inherently limits exposure to fraud, identity theft, and cargo theft.

Public load boards operate under a very different model. Platforms are accessible to a far broader audience, including unvetted motor carriers and potentially fraudulent actors. Subscription based access creates a low barrier to entry, which expands market reach but also increases anonymity. This openness has made public load boards a focal point for impersonation schemes, double brokering, and targeted cargo theft. As a result, organisations must define when such platforms may be used, what information may be disclosed, and what categories of goods are prohibited from being posted.

How risk emerges in Load Board use

The rapid growth of digital freight exchange has coincided with new avenues for exploitation. Criminal networks increasingly employ data scraping tools, machine learning, and cargo profiling methods to identify shipments of interest. Loads collected from well known distribution centres are particularly vulnerable. A posting that identifies a high value origin, even in generic form, can serve as a signal to organised thieves. Specific cargo descriptions or precise location details compound this risk.

Beyond theft, fraudulent carrier impersonation has become a major concern. Criminals may spoof phone numbers, steal motor carrier identifiers, or create convincing email domains to secure a load. Once a fraudulent party succeeds in collecting a shipment, the cargo may become untraceable in a matter of hours.

Double brokering represents another exposure, particularly when communication occurs outside formal channels. When a load is re brokered without authorisation, brokers lose visibility and control, and customers face heightened uncertainty. Payment disputes and regulatory breaches often follow. The language used in instructions can also influence legal outcomes. Communications structured as "the customer requires" or "the shipper requires" may appear to create distance from operational control, yet they also risk drawing those parties into litigation should an accident occur.

Evaluating the rationale for posting a load

Given the risks, brokers must consider the underlying rationale before deciding to post on a public load board. The nature, value, and attractiveness of the cargo should be assessed alongside customer expectations, time constraints, journey distance, and prevailing market conditions. For high value or high risk goods, load boards should seldom be the default solution. Instead, established, pre vetted carriers may offer a safer and more controlled alternative. Without such assessment, inappropriate load board use can expose both brokers and their customers to unnecessary and avoidable threats.

Managing information to reduce exposure

The most significant mitigation strategy lies in careful control of the information disclosed. While accuracy is required for safety and operational clarity, brokers should avoid providing unnecessary detail. Sensitive locations should be described in general terms without becoming misleading. Cargo descriptions should remain neutral, particularly where goods have high theft appeal. Categories such as freight all kinds, hard goods, soft goods, or perishable goods provide sufficient clarity for legitimate carriers while avoiding specific references that may attract criminal attention.

Declared weight offers another opportunity for discretion. Using a safe but generic weight, consistent with compliance requirements, may reduce the specificity of the cargo profile. While equipment type and pallet counts often need to be disclosed, these details should not be supplemented with avoidable commentary or operational notes that could reveal more than necessary.

Communication controls and identity protection

Communication practices play a pivotal role in reducing exposure to identity fraud. Using a single, centralised channel for all inbound and outbound correspondence allows for tighter monitoring, easier verification, and clearer audit trails. Organisations benefit from ensuring, so far as reasonably practicable, that communication between brokers and motor carriers occurs within the load board platform itself. Attempts to shift conversations to private phone numbers or personal email addresses may constitute a red flag and should be approached cautiously.

Software tools that validate carrier identifiers, insurance status, and safety ratings can provide additional protection. When layered with fraud detection features, they help identify mismatched contact details and mitigate impersonation attempts before they escalate.

Training and organisational governance

The effectiveness of risk management depends heavily on personnel competence. Staff who interact with load boards require training that enables them to recognise suspicious behaviour, validate carrier identities, and understand which information is sensitive. A clear escalation procedure is essential for situations that deviate from expectations or raise concerns. Without such structure, even small anomalies in communication or cargo handling may go unchallenged.

In addition, organisations benefit from establishing formal policies governing load board usage. These policies should define permitted platforms, categories of goods eligible for posting, required internal approvals, and rules regarding the content of postings. By ensuring consistency and accountability, governance frameworks transform load board use from an ad hoc operational tool into a controlled process aligned with broader risk appetite.

Conclusion

Load boards remain a critical component of the freight transportation landscape. They promote efficiency, support market flexibility, and facilitate rapid problem solving. Yet their inherent openness creates exposure to sophisticated criminal activity, impersonation, and operational breakdown. The combination of prudent information management, communication controls, structured training, and clear organisational policy forms the strongest basis for safe and effective utilisation.

Used thoughtfully, load boards can continue to support operational efficiency without compromising security. Used without adequate oversight, they can expose brokers, customers, and cargo to substantial operational, financial, and reputational harm.

Our Services: BSI Connect Screen

BSI Connect Screen is an integrated platform that employs a risk-based approach to supply chain risk management programs. It targets the biggest global supply chain threats to help organisations inspire trust and build resilience through data-driven insight. Our platform contains the largest proprietary global supply chain risk intelligence database that looks at more than 20 risk ratings in over 200 countries. BSI Connect Screen provides services and solutions to accelerate your understanding of supply chain risk and gain insight to empower decision making to build a more resilient supply chain.

These services include:

- Custom Intelligence Services
- Powerful, Interactive Risk Mapping
- Daily Updates and Notifications
- Custom Report Builder
- Supply Chain Incident Database
- Connect Screen Auditing System
- Advisory Services
- Training Services

bsi Connect Screen

consulting@bsigroup.com | bsigroup.com
1950 Opportunity Way, Suite 900, Reston, VA 20190

About TT Club

TT Club is the established market-leading independent provider of mutual insurance and related risk management services to the international transport and logistics industry. TT Club's primary objective is to help make the industry safer, more secure and sustainable. TT Club's Loss Prevention function is committed to the ongoing development of advice and information underpinning this objective.

This includes:

- Providing support to reduce the risk of claims occurrence
- Promoting 'best practice' opportunities
- Helping to improve risk assessment, mitigation, and control

Theft remains a top five area of claims cost in TT Club's global claims analysis. Analysis of incidents, increased data sharing agreements, collaborations, and widespread dissemination of findings, all serve to improve understanding of the underlying risks. This report demonstrates TT Club and BSI Consulting's shared goal of educating the transportation and manufacturing sectors about the dynamic cargo theft risks present globally.

With enhanced awareness of cargo crime trends, the industry will be able to engage in a proactive approach in preventing cargo crime, while minimising the resulting financial loss and brand reputation damage.

Highlighting risk, reducing exposure.
Advising insureds, serving the industry

Michael Yarwood
Managing Director, Loss Prevention
michael.yarwood@thomasmiller.com

Josh Finch
Logistics Risk Manager
joshua.finch@thomasmiller.com

TT

riskmanagement@ttclub.com

TT bsi

ttclub.com

bsigroup.com