BSI Consulting and TT Club 2024 Cargo Theft Report

April 2025

Your partner in progress

Table of Contents

Introduction **2**

Global cargo theft trends **3**

Strategic theft risks and America's breakdown **6**

Case study: Scams a growing risk for supply chains 7

Rail theft in the United States **8**

Case study: Organized criminal groups targeting in-transit trains in California and Arizona 9

Theft risks in South Africa **10**

Case study: Metal thefts in South Africa 10

Theft trends in Europe **11**

Case study: Rollover thefts in Europe 11

Pilferage, insider participation, and pharmaceutical thefts a risk in India **12**

Violence and hijackings a continuous threat in South America **13**

Risk mitigation strategies from BSI Consulting and TT Club **14**

Operational assessment 15

Due diligence 16

Internet enabled crime 17

Red flags 17

Our services **18**

@2025 BSI. All rights reserved.

Introduction

BSI Consulting and TT Club have collaborated to deliver an annual cargo theft report, offering a strategic analysis of global cargo theft data to uncover criminal activity and emerging threats to the supply chain. By reviewing data collected throughout the year, we provide insights into how shifting threats are transforming the logistics landscape.

The supply chain operates within an ever-changing risk environment influenced by macroeconomic factors, geographic conditions, commodity prices, economic policies, and fluctuating freight volumes. In response, criminal groups are adapting their strategies, leveraging increased organization, a deeper understanding of supply chain operations, advanced technology, and sophisticated countermeasures to target cargo with greater precision. These risks and criminal adaptations underscore the importance of this report in providing actionable insights to safeguard the global supply chain.

@2025 BSI. All rights reserved.

Global cargo theft trends

2024 cargo theft trends reveal a rapidly evolving landscape shaped by shifting criminal tactics and emerging targets. Food and beverage products were the most frequently stolen, accounting for 22% of all incidents, followed by agricultural goods at 10%, electronics at 9%, and fuel at 7%. 76% of thefts involved trucks and in terms of theft types, hijackings led at 21%, followed by vehicle theft at 20%, theft from facilities at 16%, and theft from vehicles at 14%.

The majority of thefts—41%—occurred during transit, with 21% linked to warehouses and smaller percentages attributed to production facilities, delivery sites, parking lots, and others. Geographically, hotspots included Brazil, Mexico, India, the United States, Germany, Chile, and South Africa, with the highest number of incidents reported in the first and last quarters of the year.

A standout trend this year is the growth of strategic thefts, now representing 18% of all incidents in the United States. Deception, fraud, and advanced planning define these thefts. Criminals employed tactics such as impersonation and document forgery and even leveraged AI technologies to manipulate bills of lading and orchestrate remote operations. Such schemes highlight the increasing sophistication of criminal networks and their deepening knowledge of supply chain vulnerabilities. Warehouses and transit points remain particularly vulnerable to these well-coordinated attacks.

Internet-enabled crime has also emerged as a significant facilitator of cargo theft. Criminals are utilizing artificial intelligence (AI) to create phishing emails, deep fakes, and malware aimed at accessing sensitive freight information. Reports of attacks targeting cloud-based storage services have risen, reflecting the adaptive nature of these threats. As strategic and internet-enabled thefts grow in prevalence, they emphasize the need for companies to invest in advanced security measures and robust risk management practices to protect their operations.

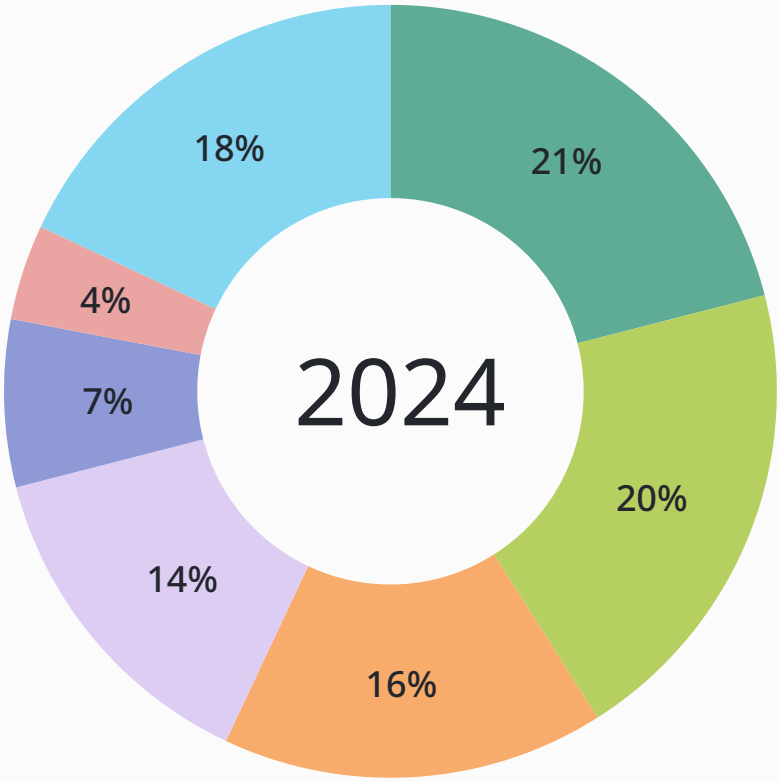
@2025 BSI. All rights reserved.

Global Cargo Theft Trends 2024

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

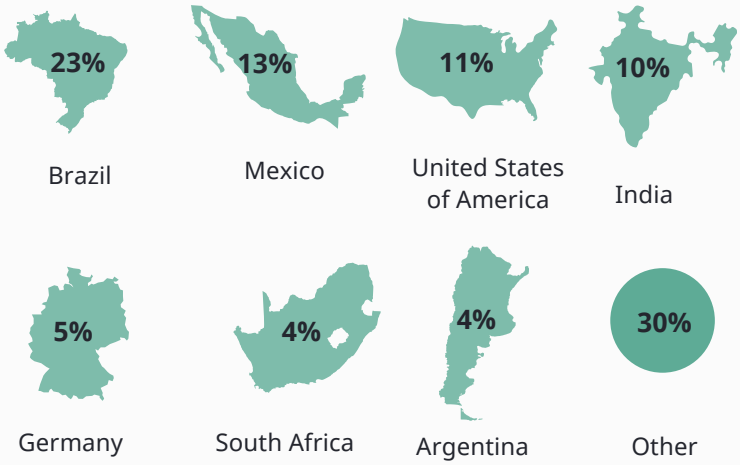
- Hijacking
- Theft of Vehicle
- Theft from Facility
- Theft from Vehicle
- Theft from Container/Trailer
- Theft by Employee
- Other



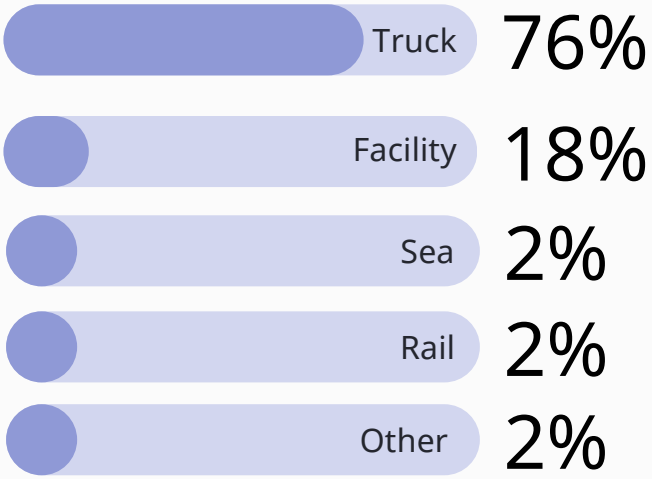
Top Commodities Stolen

22%	10%	9%	7%	5%	5%	42%
Food and Beverage	Agriculture	Electronics	Fuel	Automotive	Construction Materials	Other

Top Countries for Cargo Theft



Modalities of Theft

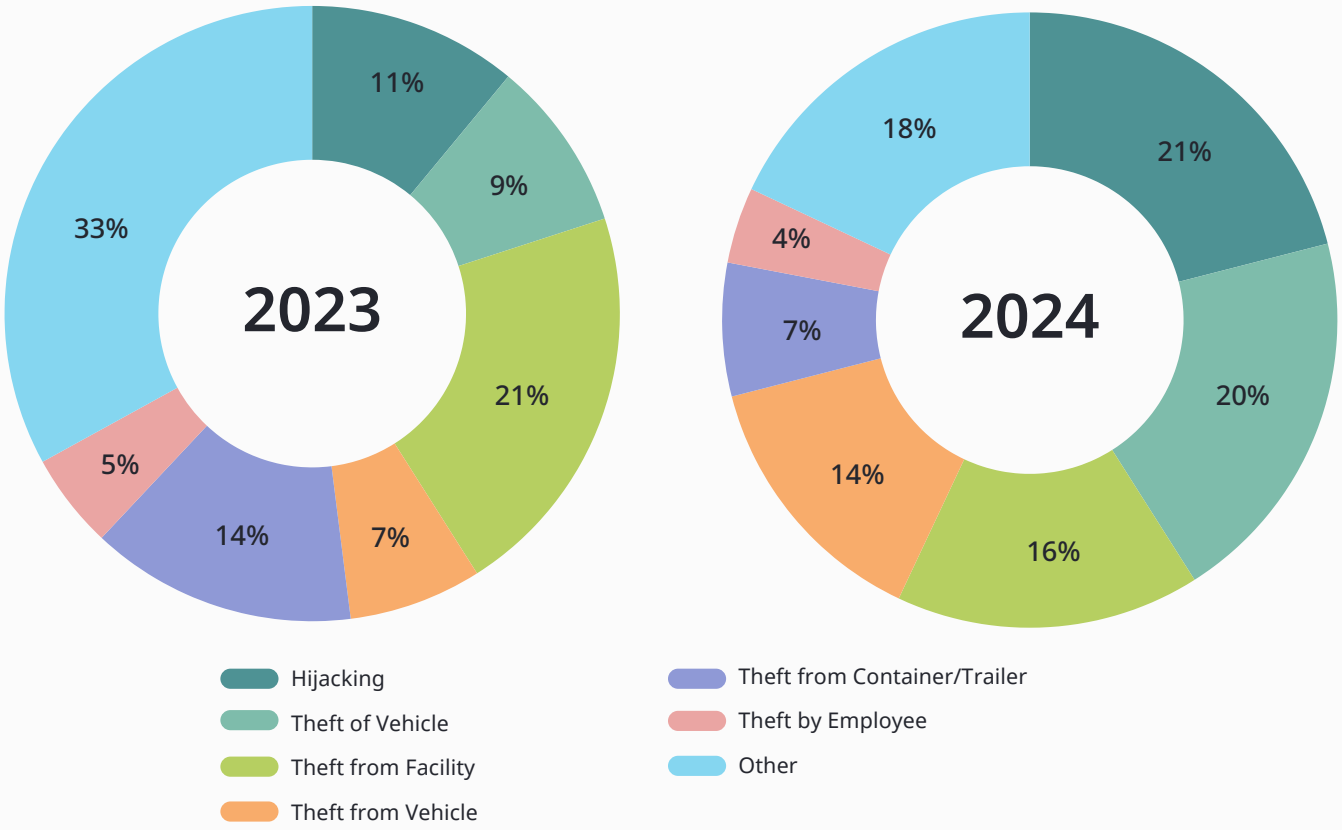


@2025 BSI. All rights reserved.

Global Theft Trends 2023 vs. 2024

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

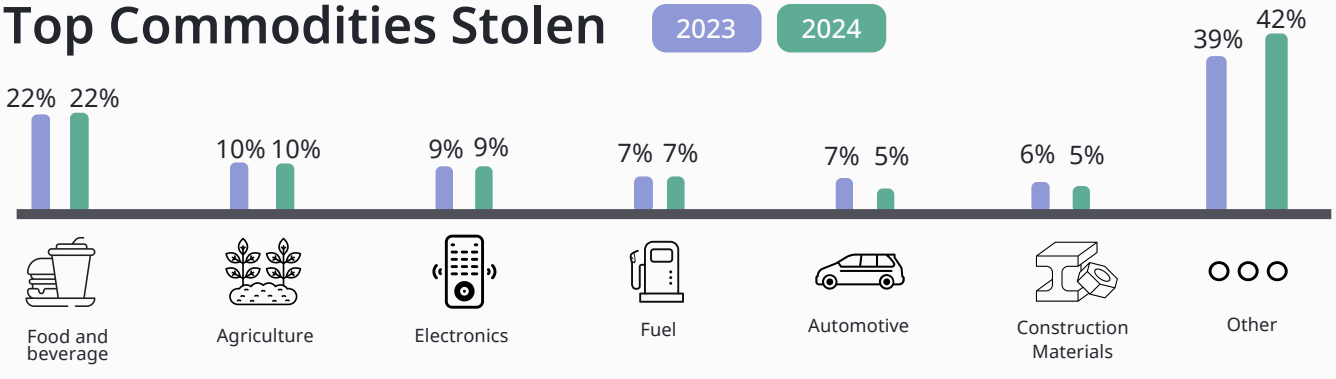


Modalities of Theft

- Truck
- Facility
- Sea
- Pipeline
- Rail
- Other

						Other
2023	68%	26%	2%	2%	1%	1%
2024	76%	18%	2%	1%	2%	1%

Top Commodities Stolen



@2025 BSI. All rights reserved.

Strategic theft risks and America's breakdown

Cargo theft trends in the United States indicate a unique and concerning pattern compared to other regions, driven by the prevalence of strategic theft methods, heightened technology vulnerabilities, insider involvement, and the targeting of high-value goods such as electronics, pharmaceuticals, and consumer products. These factors highlight the challenges of safeguarding supply chains in the face of increasingly sophisticated criminal tactics.

In the United States, electronics lead the list of stolen products, accounting for 19% of thefts, followed by food and beverages, alcohol, and parcels. The majority of thefts occur during transit, with trucks the primary target 79% of the time, followed by incidents at facilities at 13%.
In recent years, the United States has witnessed a surge in strategic cargo theft, which now accounts for approximately 18% of all incidents.

These thefts are characterized by the use of deception and advanced technological expertise, enabling criminals to execute highly coordinated schemes. High-value goods, such as electronics, apparel, and pharmaceuticals, are particularly vulnerable to these tactics, as organized crime groups continue evolving their methods to exploit supply chain vulnerabilities.

While California initially emerged as the epicenter of strategic cargo theft, the problem has since expanded across the United States. Incidents are broadening, with reports of these thefts occurring in Illinois, Indiana, Ohio, Kentucky, Louisiana, and Pennsylvania. This geographic spread reflects the growing reach of organized criminal networks and the emergence of new actors leveraging fraudulent techniques. Industries ranging from food and beverage to metals, consumer goods, and apparel have all experienced the impact of strategic theft.

This problem is exacerbated by insider participation, with criminals leveraging access to sensitive information to identify and intercept high-value shipments. Internet crime also plays a pivotal role in modern theft schemes, enabling bad actors to exploit technological vulnerabilities for fraudulent gain. The combination of these factors has made cargo theft a dynamic and ever-evolving risk for supply chain stakeholders.

@2025 BSI. All rights reserved.

Case study: Scams a growing risk for supply chains

Scams and fraudulent activity have increased over the last years. The COVID-19 pandemic resulted in a shift towards a more digitised world with volumes of online shopping, banking, and general transactions increasing dramatically.

Effective strategies that facilitate mainstream frauds inevitably evolve and are put to good use by the criminals targeting the supply chain. Some estimates suggest that online fraud is a US$500bn global industry which places it on a par with illegal drugs in terms of scale.

Computer misuse crimes involve unauthorised access to systems and data. Whether it be transport management systems, warehouse management systems, or general communications, the supply chain relies heavily on IT systems to drive efficiency of operation. This provides multiple valuable data sources for criminals to infiltrate and gain access to cargo.

This activity is cost effective for the criminals, requiring little more than a phone line and internet connection they are empowered to act on a global basis with no physical constraints. As with cargo crime generally, barriers to entry are few and the potential returns are high.

In the fast-paced supply chain business environment, a simple pause and assess protocol could serve to identify an attempted fraud before it is too late.

@2025 BSI. All rights reserved.

Rail theft in the United States

Cargo theft from trains remains a persistent and growing concern in the United States, accounting for approximately 6% of all reported thefts in 2024, a significant increase from 3% in 2023. Criminals are becoming more strategic in their methods, with groups in California exemplifying this trend by leveraging their understanding of train schedules and exploiting shift changes among rail staff to execute thefts with alarming efficiency.

Modalities of Theft in the US

- Truck
- Facility
- Rail
- Van
- Sea

2023	79%	14%	3%	3%	1%
2024	79%	13%	6%	2%	0%

Southern California, with its high volume of cargo from the region's ports, is particularly vulnerable. Slow-moving trains in cities like Los Angeles are easy targets for theft, especially due to a lack of adequate security personnel and antiquated locks. This vulnerability is not unique to California; theft risks extend to Illinois and Tennessee, where rail terminals and switching yards serve as prime targets. Here, containers often remain stationary for extended periods, and security measures are frequently inadequate. **Unlike truckload shipments, which are usually monitored by drivers or security, rail cargo often lacks consistent oversight during transit, providing thieves ample opportunity to operate undetected.**

The types of goods targeted reflect high-value priorities for criminals, with electronics being the most stolen, followed by automotive parts and footwear. In response to these challenges, companies are exploring advanced technologies to mitigate risks, including real-time tracking systems, ISO-compliant seals, and mobile security units. These solutions offer a more tailored approach to protecting specific locations and cargo types, aiming to stay ahead of increasingly organized and opportunistic criminal operations.

@2025 BSI. All rights reserved.

Case study: Organized criminal groups targeting in-transit trains in California and Arizona

Authorities believe that an organized criminal group operating out of Sinaloa, Mexico is targeting trains for theft in rural areas as they travel with goods from California toward Arizona. Evidence suggests criminals are targeting in-transit trains, climbing aboard the trains while they are stopped at a staging area. They have also been known to interfere with a train's braking system or signal boxes, forcing the train to stop.

This method not only results in physical damage to the train but also puts the safety of the train workers at risk. Other criminals follow the train in vehicles they use to carry the stolen merchandise.

The theft incidents demonstrate that the thieves have sophisticated operations, leveraging intelligence on shipments such as the use of locks and other security measures to target high-value goods, including electronics, footwear, and tools. This shift to more rural theft incidents is likely tied to more opportunity for criminals to commit theft without being detected. Even when train employees witness the thefts occurring, company policy discourages worker intervention to prevent injury if thieves are armed.

@2025 BSI. All rights reserved.

Theft risks in South Africa

South Africa ranks among the top countries globally and leads the African continent in cargo theft incidents, highlighting the significant economic impact of this persistent issue. Trucking remains the most commonly targeted mode of transportation, with hijackings of loaded trucks being the predominant method. These often-violent incidents involve well-organized gangs employing tactics such as intercepting stationary vehicles or posing as police officers to force trucks to stop. In addition to trucking, thefts from warehouses, as well as rail and air freight robberies, are also prevalent. The top regions for cargo theft in 2024 were Gauteng, KwaZulu-Natal, Eastern Cape, Mpumalanga, and Western Cape.

Employers must remain vigilant against the risk of insider participation, as corrupt employees can directly assist with thefts or provide criminals with sensitive information about shipping schedules and security protocols. Instances of faked hijacking reports and the involvement of security guards hired for protection further complicate mitigation efforts. The most stolen products in 2024 included food and beverages, parcels, animals, alcohol, and fuel, reflecting the diversity of targeted goods. Proactive measures, such as enhanced employee vetting, improved security protocols, and investment in advanced technologies, are critical to addressing this multifaceted challenge.

Case study: Metal thefts in South Africa

Over several years we have witnessed thefts of various metals, typically these high value shipments are targeted on the road leg of their transit heading for the export port. Often these shipments are containerised and are transported over significant distances. The attack frequently involves a hijacking of the truck, potentially with the use of force and violence.

A concerning aspect of a recent incident was insider involvement that facilitated cargo access. The initial transport, arranged by the shipper, included weighing the cargo at both the manufacturing site and the receiving facility, with an independent third party verifying it before export. However, nine container loads, collected over several days, never made it to the export port.

Investigation revealed that cargo theft had been a known issue at the facility, and inventory management vulnerabilities allowed manual entry of data, which delayed reconciliation. This created a window for cargo to be removed without immediate detection. Furthermore, no due diligence checks were conducted on the trucking providers used.

Poor security practices at the facility enabled small-scale exploitation, eventually escalating into an organized criminal operation. Gang members offered cash rewards to staff for access to information and the cargo. As a result, nine trucks were allowed to collect containers, which were never recovered.

@2025 BSI. All rights reserved.

Theft trends in Europe

Cargo theft in Europe remained relatively stable compared to previous years. High-demand goods such as food and beverages (12% of thefts), electronics (12%), metals (9%), and alcohol (7%) were the most targeted commodities, with an overall increase in cargo theft incidents reflecting ongoing vulnerabilities within Europe's supply chains. Organized criminal groups continue to exploit the appeal of easily resold items, underscoring the need for enhanced security measures across the industry.

Warehouses were the most targeted locations, accounting for 41% of recorded incidents. Thefts at rest areas, parking lots, and unsecured roadside locations also constituted a significant portion of the incidents. Common tactics included theft from facilities, containers, and trailers, as well as vehicle hijackings and "slash-and-grab" methods.

Countries such as Germany, the United Kingdom, Italy, Spain, and France experienced the highest rates of theft, with parked vehicles in unsecured rest areas and poorly secured warehouses serving as primary targets. Notably, technologically sophisticated thefts are on the rise, echoing trends in the United States. For example, a shipment of copper bolts in Austria destined for France was diverted by criminals using false delivery instructions, resulting in mid-six-figure USD losses.

The risk to drivers also remains a serious concern. In one notable case near Milan, Italy, a gang was arrested for targeting truck drivers during their mandatory rest stops. These incidents often involve a variety of tactics, such as slashing tarpaulins of soft-sided trailers, breaking locks, or violent tactics such as injuring or kidnapping drivers. Such examples illustrate the growing complexity and danger of cargo theft in Europe, emphasizing the urgent need for stronger security protocols, driver training, secure rest areas, and investments in technology to protect assets and personnel.

Case study: Rollover thefts in Europe

Criminals are known to have accessed the cargo space of trucks on the move for a number of years across Europe and beyond. Of all the strategies they employ to infiltrate the supply chain, rollover thefts present the highest risk to those involved.

Learn more: View rollover theft animation

A number of these types of incidents across Europe and the United Kingdom have occurred over the last twelve months. Aside from the obvious danger, these crimes are particularly challenging to investigate, given that the truck driver and their records typically show no evidence of an unauthorised stop during their journey and no obvious point at which the cargo was stolen. It is only at the delivery point that the theft is identified, that might be several days away and by which time the cargo and criminals are a significant distance away.

Criminals will go to great lengths to prepare for such an attack, ensuring the target truck and cargo are worth the risk. Thieves may recruit insiders—such as warehouse staff to plant GPS devices, dispatchers to confirm cargo, or truck drivers to minimize risk during the attack.

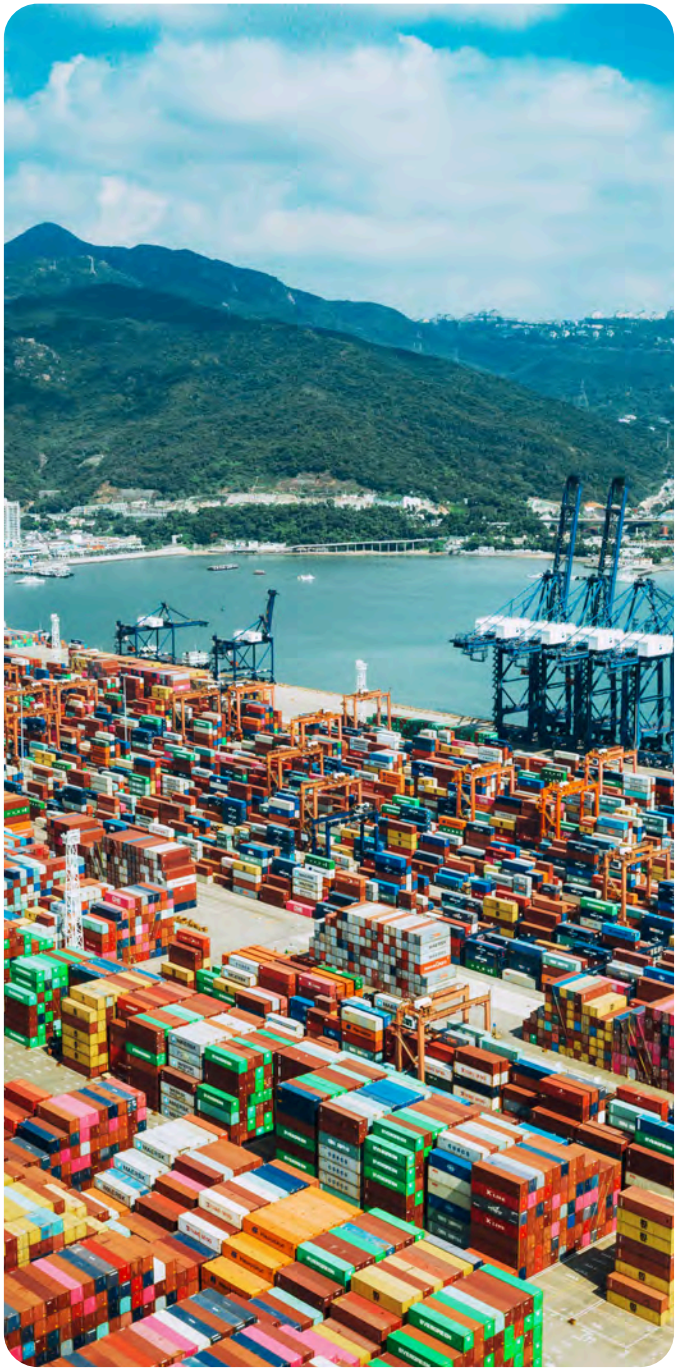
Mitigating this threat can be approached on several levels. Awareness of insider threat would be prudent and robust steps put in place to mitigate the identified risks.

- Awareness of and training to identify insider threat
- Robust information management
- Driver training and awareness

@2025 BSI. All rights reserved.

Pilferage, insider participation, and pharmaceutical thefts a risk in India

There are a variety of different risks to cargo across India. The states of Uttar Pradesh, Madhya Pradesh, Rajasthan, Haryana, and Bihar were among the hotspots for cargo theft last year. Cargo theft poses significant risks to supply chains, driven by insider involvement, opportunistic pilferage, and targeted theft of high-value goods like pharmaceuticals.
A substantial proportion of cargo thefts in India involves insider participation, with BSI Consulting data revealing that at least 26% of incidents in 2024 were linked to insiders. Corrupt warehouse employees often collude with theft gangs, sharing security protocols that allow criminals to bypass safeguards. These employees may also coordinate with truck drivers to load excess cargo and falsify records, enabling systematic thefts that accumulate into significant losses over time. Insiders can manipulate operational vulnerabilities, making their actions particularly damaging to supply chain integrity. This type of theft, coupled with the risk of violent external raids, demonstrates the multifaceted nature of cargo theft challenges in India and the critical need for enhanced employee screening and security oversight.



In India, pilferage continues to be a persistent threat. While incidents of theft vary in scale, the risk is amplified by inadequate security measures such as the use of tarps, which serve as mere visual deterrents. The top products stolen across India in 2024 were Food and Beverage, Agriculture, and Electronics. Overnight parking in unsecured locations like gas stations exposes goods to opportunistic thieves who exploit these gaps. Additionally, subpar road infrastructure and driving behaviors create scenarios where overturned trucks or slowed vehicles become easy targets for theft, further compounding the challenge of safeguarding cargo.

As one of the world's largest producers of pharmaceuticals, India faces a unique risk from targeted cargo theft in this high-value sector. The theft of pharmaceuticals is infrequent but deeply impactful, as evidenced by three incidents recorded in December 2024. Two in-transit cargo trucks and one parked truck without proper security were targeted, emphasizing the need for improved protective measures. These incidents underscore vulnerabilities in the transportation process, where inadequate measures like tarps and unsecured parking create exploitable points of failure. Compounding this issue is the prevalence of corrupt drivers who occasionally stage hijackings, making it difficult to assess the true scope of the problem. With pharmaceutical shipments being critical to global health supply chains, the stakes of addressing these risks are exceptionally high.

@2025 BSI. All rights reserved.

Violence and hijackings a continuous threat in South America

In 2024, South America faced significant challenges with cargo theft, with Brazil the epicenter, accounting for 68% of recorded incidents in the region. Argentina, Chile, and Peru followed, with Argentina holding the second-highest proportion of thefts at 12%. Hijacking remains the most prevalent theft method, constituting 33% of all cargo theft incidents. Criminal activity in the region is often violent, with truck drivers routinely threatened, assaulted, kidnapped, or killed.

Technological advancements have become both a tool and a battleground in the fight against cargo theft in South America. GPS systems and engine immobilizers enable companies to track and disable stolen vehicles, aiding in the recovery of shipments. However, criminals are adapting, employing GPS jammers to block location tracking and even hacking carrier accounts to orchestrate fictitious pickups. Throughout 2024, BSI Consulting recorded several instances in Brazil of criminals effectively leveraging these technologies.

The region's economic and infrastructural challenges further exacerbate cargo theft risks. Poorly maintained roads in countries like Brazil, Argentina, and Chile contribute to frequent truck overturns, prompting opportunistic pilferage by local residents. Meanwhile, Argentina's economic crisis could fuel a rise in criminal activity, as constrained opportunities push individuals toward theft. Additionally, the growing presence of drug smuggling gangs in Ecuador threatens to destabilize security, potentially driving an uptick in other crimes, including cargo theft. As these dynamics unfold, companies must remain vigilant and adaptive to protect their supply chains in an increasingly complex environment.

@2025 BSI. All rights reserved.

Risk mitigation strategies from BSI Consulting and TT Club

BSI Consulting and TT Club have created this report to analyze emerging trends and threats to the supply chain through 2024 and into 2025. We offer the following mitigation strategies to help organizations proactively understand risks and develop more resilient supply chains.

Recommended mitigation methods to counter thefts:

- **For freight exchange/load board facilities:** Consider the details you are disclosing and how this might be attractive in the wrong hands. Beware of unusually attractive offers. Perform robust vetting on carriers outside of the platform.
- **For drivers/carriers:** Ensure they have mapped out routes to identify the safest parking locations available. Ideally, these would be well-lit, fenced, with staffed access gates. Review high-risk areas along the route and designate “no stop” areas.
    - Information management and risk assessment is vital to identify which data holds the greatest risk and then develop strategies to protect that data. Routing information and GPS data could be invaluable to the criminal seeking to access cargo during transit - share only on a need-to-know basis.
- **For email communications:** Be vigilant, don’t open emails or attachments from contacts you don’t know. Raise awareness of the risk through phishing training. Educate all personnel. Email addresses may be masked so that they appear to come from a legitimate source. If you receive an email communication from a known contractor which asks you to reply to a different email address, it is a red flag.
- **For inventory management:** Tight controls over held inventory are essential to mitigate the risk of skimming. Regular rolling stock checks provide an additional deterrent, as well as control over access rights to the system.
- **For goods receiving:** Check if the signed delivery note evidences the volume of goods you have delivered or received. Manipulation of paperwork can facilitate unfettered access to cargo and allow criminals to access large volumes over time. Goods received should be scanned into the inventory management system and not received in bulk.

@2025 BSI. All rights reserved.

Recommended mitigation methods to counter strategic and fraudulent thefts:

“If it is too good to be true, then it probably is.”

Operational assessment
A fundamental starting point is to understand your operational requirements. This could include:

- Average volumes of cargo to be transported
- Typical collection and delivery locations
- Seasonal variations driven by demand (peak and trough)
- Average number of truckers available
- The intended use of load boards (should be used with caution)
- Confirmed cargo values are at or below customer contract limits before shipment acceptance and carrier assignment

Understanding these needs will provide opportunity to risk assess and set a robust strategy. This assessment will naturally be unique to each stakeholder and will result in different demands when managing security.

Operational demand will assist in forming strategies such as manual versus automated processes. There might be an upfront and ongoing cost associated with automated systems, but these could be rationalised when comparing personnel hours to perform the task manually and assessing how robust the manual process is. Outsourcing could be another consideration where due diligence is concerned, again driven by demand.

Where appropriate, it might be prudent to narrow down the number of “approved” trucking companies that you routinely do business with. Maintaining full due diligence on 1,000’s of trucking companies is practically going to be more difficult than 100’s. It is almost certainly going to be more difficult to identify the typically small changes in behaviour of a trucking company that you employ infrequently.

@2025 BSI. All rights reserved.

Due diligence

Once an overarching strategy has been established then robust due diligence processes need to be established. These processes will look different depending on the size of your company, they should be proportionate to the assessed risk but importantly should always be followed. It should be assumed from the outset that there will be anomalies, and a fundamental component of the due diligence process should be appointing a small number of individuals with sufficient authority to make time sensitive decisions at business level. A clearly defined escalation procedure should be established as a priority and should consider periods of peak volume, out of hours periods and holidays to ensure 24/7/365 coverage.

- **Screening and vetting –** these services could be manual and performed internally by trained personnel, could be outsourced entirely or a hybrid solution could be introduced whereby a third-party solution provider closely interacts with the business to ensure best outcomes.
- **Central databases –** there are several central databases through organisations such as Registry Monitoring Insurance Services (RMIS) and Federal Motor Carrier Safety Administration (FMCSA/Safer) that could be interrogated for relevant risk related information.
- **What processes and procedures do the trucking company have in place as an additional layer of security?** Technology such as Electronic Logging Devices (ELD's) could be explored, however, it would be prudent to seek legal advice defining the requirements contractually.
- **Standard operating procedures –** these could be established to require trucking companies to provide a list of their tractor VIN numbers. These could be used in security checks when the driver arrives to collect the load to ensure that the cargo is only released to the expected truck driver. While VIN number is preferable, something more basic such as the Motor Carrier number displayed on the tractor, the make and year of the tractor, and trailer number could add an additional layer of security.
- **Rules based approach –** through the vetting process using available databases, rules could be established for example to include a requirement that truckers have been in business for a minimum of 1 year and that business information cannot have been changed on the FMCSA website for at least 6 months. A rules-based approach could assist in avoiding fraudsters who have either just set up the business or who are impersonating a legitimate trucking company.
- **Monitoring and response –** there are numerous track and trace technologies that can prove effective as an added layer of deterrent. Such solutions do not necessarily solve the security risk, however where they are in place, businesses should consider how and who is monitoring the data feed and what a proportionate response to a breach would be. Criminals should not be underestimated, time is on their side, there are many cases where we have seen evidence of penetration testing and if the response is not effective when a security alert is triggered then the criminals will typically continue their operations as if the technology didn't exist.

@2025 BSI. All rights reserved.

Internet enabled crime

Business email compromise is a perennial challenge for all businesses. The strategies employed by the criminals are extremely effective and in the absence of awareness training and software solutions, the criminals' job is made easy. There are several risk mitigation strategies that could be considered to reduce the risk of being caught out by this approach.

- **Vigilance –** particularly for smaller businesses, it is likely that a sophisticated automated solution will be cost prohibitive. It is vital in such circumstances to ensure that a robust manual procedure is in place to check and verify inbound email addresses, to identify and question anomalies and changes to agreed plans. It is essential in such circumstances that personnel who are responsible for tendering cargo have adequate awareness training and understand the escalation procedure. Any triggers of suspicion should be reported to designated person(s) for further review.

- Load boards have the potential to attract criminals, consider the details you are disclosing and how this might be attractive in the wrong hands. Beware of unusually attractive rate offers and high capacity from a single source. Perform robust vetting on carriers outside of the platform.

- **IT solutions –** there are a variety of sophisticated IT solutions that could be considered to provide a more comprehensive layer of protection to your business. Such solutions can be installed and work in parallel to packages such as Microsoft 365 and will work seamlessly to protect your business from different related threats that could be tailored to your specific needs. Such solutions could automatically raise red flags in situations including:

    - **Typo squatting –** this typically manifests in a small change to a recognised email address. The criminals' hope is that the change goes unnoticed allowing them to correspond with you as if they were the trucking company.

    - **Bannering –** this involves identifying newly created or unusual email domains. Typically, when adopting this type of strategy, the criminals will identify a target and create a new email domain to facilitate the correspondence, once the cargo has been stolen, the newly created domain is closed-down.

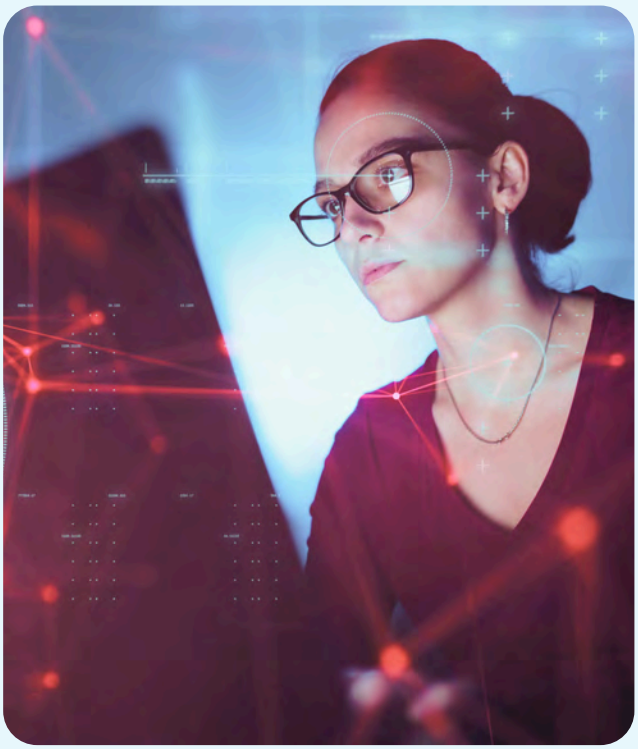
    - **Blocking IP addresses –** it is often considered that due to the remote nature of this type of attack that the criminals could be corresponding from another country. It could be possible to define which countries you routinely work with and block all email traffic originating from any other country.

    - **Domain-based Message Authentication, Reporting, and Conformance (DMARC) –** can assist in preventing the use of domain copying.

    - **Phishing, spearfishing, business email compromise –** using AI based language tools it is possible to identify and match writing styles, identify who the parties are and establish whether prior contact has been made.

A related concern is where criminals access and digitally amend genuine centrally held records. Being aware of this risk is prudent and then periodically checking for changes made can assist in identifying criminal intent. Simple queries such as how long has the trucker been on the database, were the changes made of significance could be sufficient to identify a threat.

As with due diligence procedures, it is critical to ensure that IT systems and related processes incorporate alerts, red flags and hard stops when original carrier information has been changed by even one character. Defining an appropriate escalation process and communicating who within the business has the authority to make business level decisions to override established processes is crucial.



Red flags

There is no one-size-fits-all solution to mitigating this risk. The list below has been compiled from claims examples through 2024 where cargo was stolen and could be incorporated into your security strategy as a series of red flag indicators.

- Free mail email accounts – these accounts can be created and deleted with ease
- Truckers that only use mobile phone numbers
- No website
- Past commercial disputes
- Longer range shipments
- Spot hire contracts
- Double brokering
- Downturn in economy
- High risk cargoes (develop an understanding of at-risk commodities)

@2025 BSI. All rights reserved.

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 organizations 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

Contact BSI Connect Screen's Intelligence Analysts

Jason Willoughby
Jason.Willoughby@bsigroup.com

Anna Lee Robbins
AnnaLee.Robbins@bsigroup.com

Stephanie Phillips
Stephanie.Phillips@bsigroup.com

Heather Mullen
Heather.Mullen@bsigroup.com

Millena Kiros
Millena.Kiros@bsigroup.com

Emily Lewis
Emily.Lewis@bsigroup.com

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 and more secure. TT Club's Risk Management team 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

@2025 BSI. All rights reserved.

Your partner
in progress

@2025 BSI. All rights reserved.