

2021 Cargo Theft Report

TT CLUB,
TAPA EMEA
and BSI Connect
SCREEN Intelligence



TABLE OF CONTENTS

01

Introduction

02

Global Cargo Theft Trends

03

Increased Idle Times and the Related Risks

04

Unpacking the Global Risk of Insider Theft in 2021

05

Criminals Adopting Tactics to Target the Changing Environment for Freight Transportation

06

Organizations Have Been Forced to Abruptly Adapt their Supply Chains – What to know as this trend continues

07

Case study: Increase in railfreight thefts due to factors such as port congestion, is an increased weakness in supply chain security, as highlighted by this case in the Los Angeles area



INTRODUCTION

BSI publishes this report in coordination with TT Club and TAPA EMEA. BSI Supply Chain Services and Solutions is the leading global supply chain intelligence provider, auditing services, audit & risk management compliance solutions, and advisory services. BSI's charter is to help corporations, governments, and associations identify, manage, and mitigate global supply chain risks and maintain world-class governance, risk, and compliance programs. BSI's holistic supply chain risk management suite is designed to predict and visualize risk and develop robust risk mitigation and compliance management programs to protect global supply chains, brands, and reputation. BSI's intelligence-infused supply chain solutions and global network empower the clients to understand global supply chain risk with unequaled precision.

TT Club is the established market-leading independent provider of mutual insurance and related risk management services to the international transport and logistics industry. The Club's services include specialist underwriting, claims management, and risk and loss management advice, supported by a global office network. TT Club's primary objective is to help make the industry safer and more secure. Established in 1968, TT Club has more than 1100 Members, spanning owners and operators, ports and terminals, and logistics companies, working across maritime, road, rail, and air. Members range from some of the world's largest logistics operators to smaller, bespoke companies managing similar risks. The Club is renowned for its high-quality service, in-depth industry knowledge, and enduring Member loyalty. It retains more than 97% of its Members with a third of its entire membership having chosen to insure with the Club for 20 years or more. TT Club is managed by Thomas Miller - an independent and international provider of insurance, professional, and investment services.

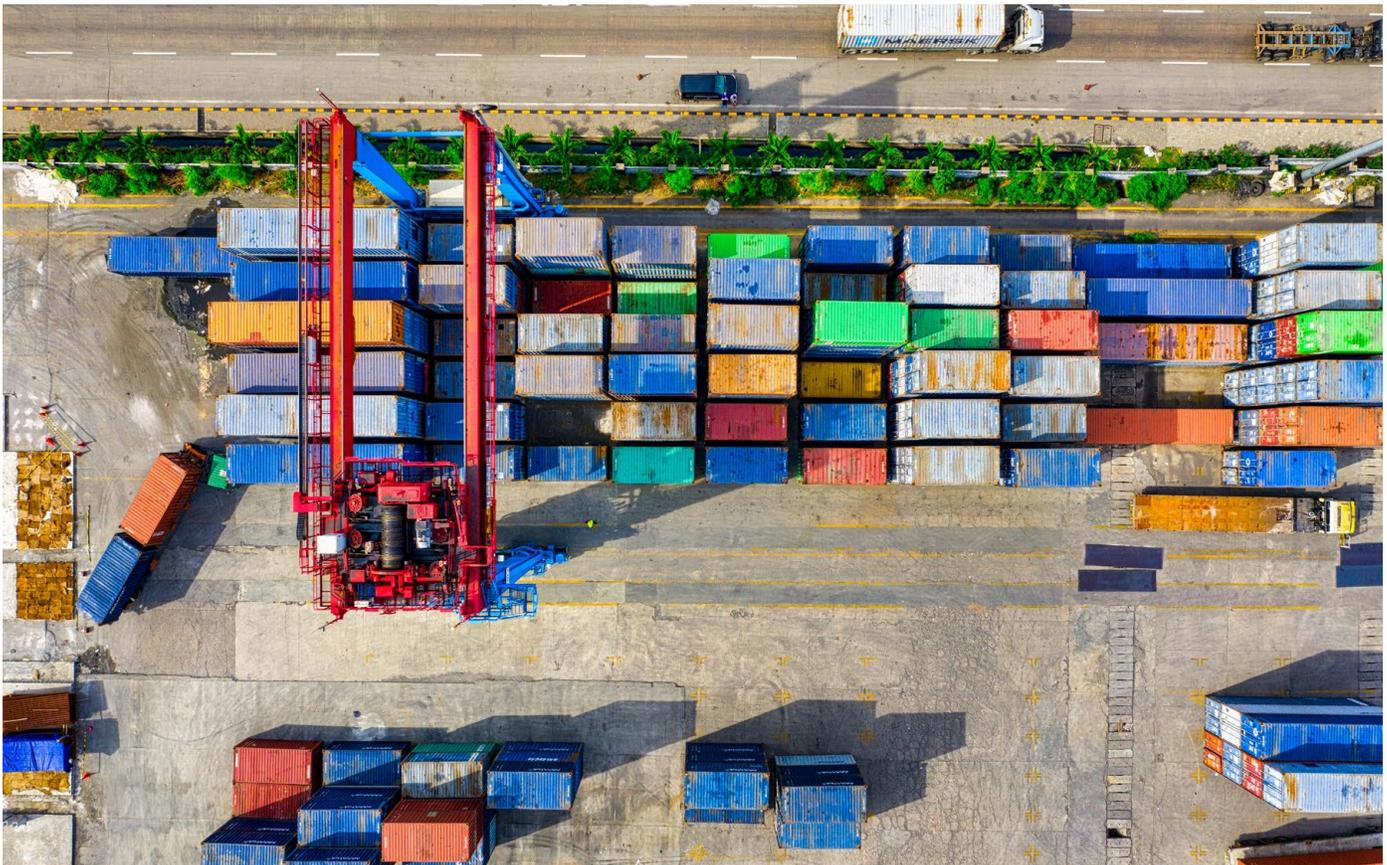
The Transported Asset Protection Association (TAPA) is a not-for-profit industry that helps Manufacturers/Shippers and Logistics Service Providers minimise losses resulting from cargo thefts and to increase the security and resilience of their supply chains. Today, in the Europe, Middle East & Africa (EMEA) region, the Association provides a host of certifiable, independently-audited industry Standards for facilities, trucking operations and secure parking as well as training. The TAPA EMEA Intelligence System (TIS) also provide the latest and historic recorded incident intelligence, enabling more secure route planning by helping members understand when, where and how criminals are targeting supply chains, and the products most frequently stolen. The Association strongly advocates the reporting of all cargo thefts to increase industry knowledge of risks and to assist companies' loss prevention strategies. TAPA EMEA's President and CEO is Thorsten Neumann. TAPA EMEA has contributed to the Europe, Middle East & Africa content of this report.



GLOBAL CARGO THEFT TRENDS

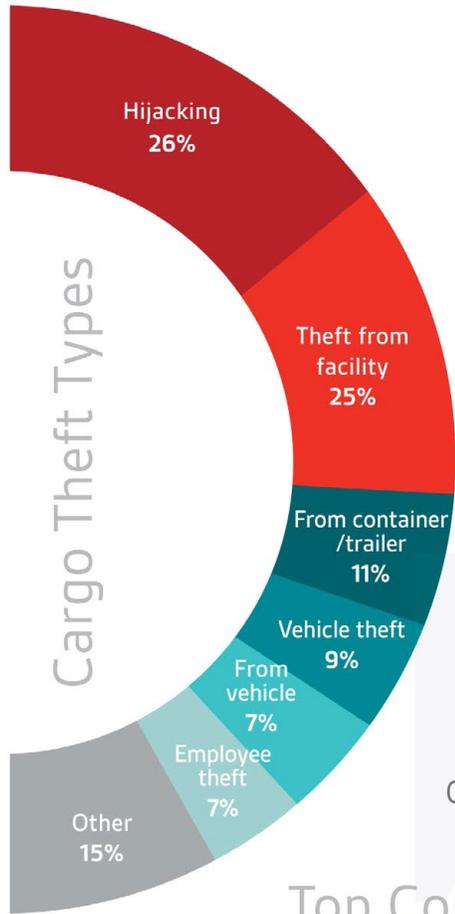
Throughout 2021, global supply chains continued to face significant security, continuity, and resiliency threats due to the COVID-19 pandemic, and although its impact seems to lessen in the early stages of 2022, it caused disruptions and major delays throughout 2021, and still has massive residual impacts globally. Many of the concerns BSI, TT Club, and TAPA EMEA monitored throughout 2021 set the tone for continued risk to supply chain security in 2022, but simultaneously new challenges and risks are likely to play a large role, such as the ongoing conflict in Ukraine which is disrupting many industries on the short-term, and could have a variety of long-term effects. This report seeks to highlight the cargo security threats that plagued supply chains in 2021 and provide organizations with mitigation techniques to combat these threats, and considers some of the emerging risks we anticipate in the upcoming months and years. BSI, TT Club, and TAPA EMEA have identified five key themes that stood out as we looked back on 2021:

- A strong increase in idle times due to significant port congestion throughout the year
- The emerging risks of insider theft
- The vulnerabilities that come with increased use of digital means by suppliers
- Consequences of an urgent need to change the locations of suppliers, and what to keep in mind during that process
- Lastly, in a case study, we unpack how cargo thefts from railway locations and trains has shown to be an increased weakness in supply chains, particularly in the region of Los Angeles in the United States.

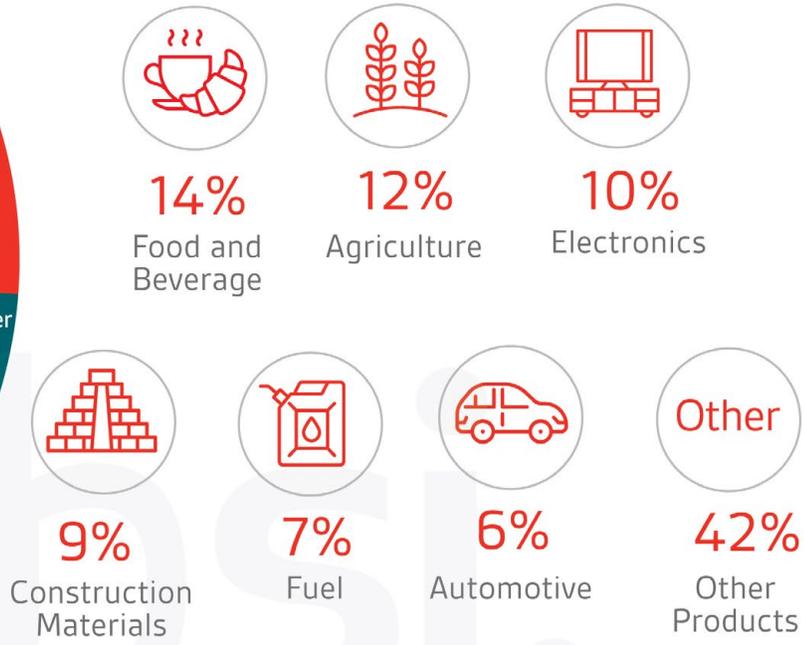


Global Theft Trends 2021

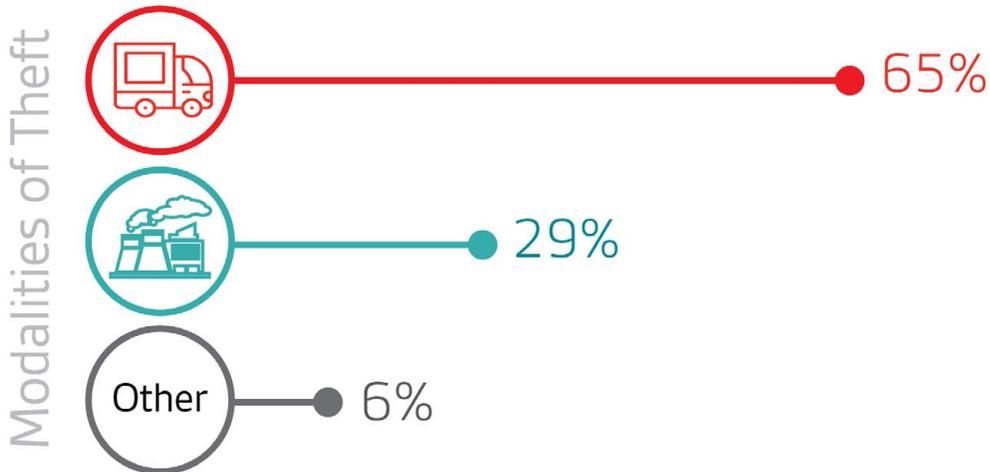
Based on recent incident data via collaboration and partnerships with law enforcement, government, non-government, commercial partners, trade associations, open-source media reports, and input from BSI advisors and expert consultants



Top Commodities Stolen



Top Countries for Cargo Theft



Global Theft Trends 2020 vs 2021

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 from Container/Trailer

 Theft of Vehicle

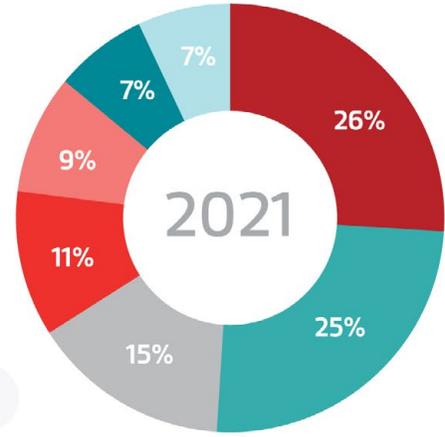
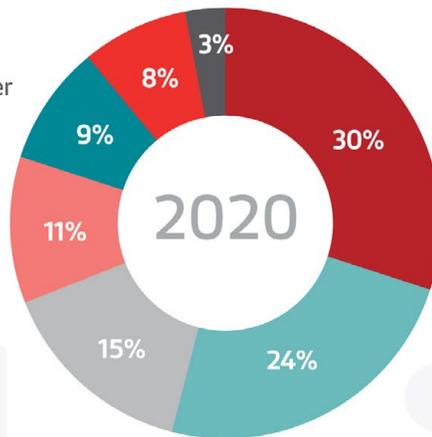
 Theft from Vehicle

 Theft from Facility

 Theft by Employee

 Slash and Grab

 Other



Modalities of Theft



Other

2020 71% 25% <1% 4%

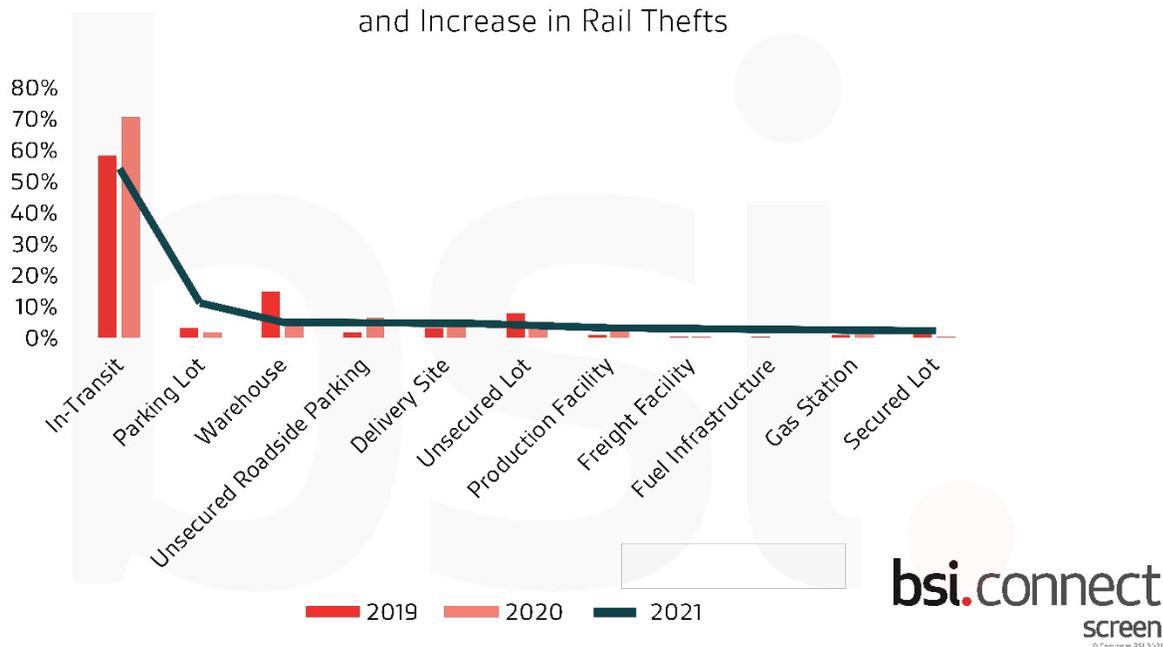
2021 65% 29% <1% 6%

A STRONG INCREASE IN IDLE TIMES LED TO AN INCREASE IN CARGO TARGETED AT REST

While actual global cargo theft incident numbers are down from 2020, in 2021, we saw a significant increase in criminals targeting cargo at rest. Whether it be at unsecured parking lots or container yards near port facilities, delays indirectly made cargo more vulnerable to tampering by thieves and smugglers. These cargo crime trends are juxtaposed with record-breaking cargo transiting through ports, driving record-breaking port congestion and idle times. These supply chain trends are furthermore symptomatic of macro-economic trends of a 'push and pull' market. Various issues emerged indirectly from this port congestion, relative to region and risk profiles. However, in this report, we will focus on cargo theft, stowaway introduction, and business continuity risks as seen in some African and South American countries.

Port Congestion in North America Linked to Diversification of Theft Types and Increase in Rail Thefts, Latin America Impacted Economically

Port Congestion in North America Linked to Diversification of Theft Types and Increase in Rail Thefts



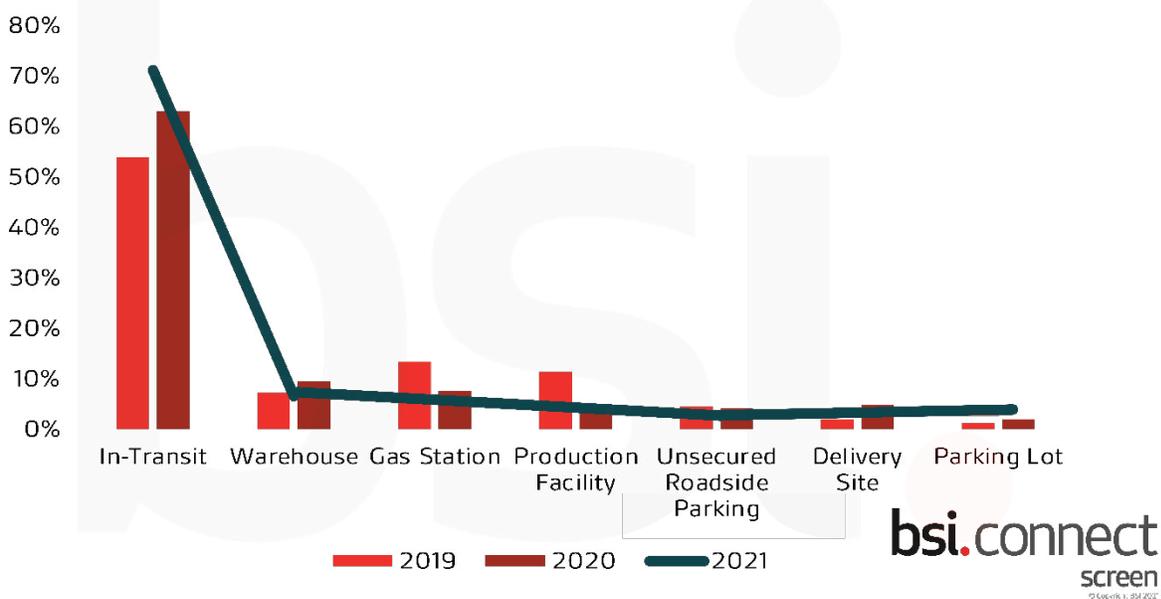
Global logistics hubs are facing a double risk with both the port congestion and spike in demand leading to train cars and cargo containers sitting idle for extended periods of time, thereby making them more vulnerable to theft. In North America, with the backlog of trains crisscrossing from the West Coast to the East Coast, trains are subsequently left parked for extended periods of time, leading to spikes in rail thefts across the United States, notably in key logistics hubs connected to local ports, like East Los Angeles in California, and in Memphis, Tennessee. This is especially the case across the United States for high-value and shortage-prone goods like electronics.

The record level of port congestion is also leading to the diversification of theft types, in 2021, as port congestion reached a record high average wait time of 17 days, containers continued to pile up at ports, leading to a variety of new cargo theft trends, particularly the diversification of theft types. For example, as warehouses are getting pushed to capacity, pivotal logistics players, like drivers, are forced to diversify where cargo is going, from secured lots at facilities, to drop lots, and eventually to unsecured parking lots due to the overflow.

This diversification of locations is similarly reflected in the diversification of theft types and locations in the United States. These cargo crime trend changes can in part be due to congestion and delays. And as Truck drivers are increasingly forced to park their trucks with the tractor/trailer/container in unsecured parking lots or outside of delivery sites due to the full secured lots, this will likely be a sustained trend parallel to the diversification of routes and modalities for logistical players due in part to the congestion.

Meanwhile, across Latin America, especially Mexico, Colombia, Brazil, Peru, and Panama, port congestion, combined with higher shipping premiums, led to fewer exports from these countries, so less cargo transiting through them in 2021.

Theft Locations as Percentage of Cargo Theft Incidents in South America
From 2019-2021



Cargo Theft and Stowaway Introduction Trends Relative to Idle Times in Europe

In Europe, continuing high levels of cargo thefts and stowaway introduction were two issues closely linked to the pressures created by increased congestion and longer idle times.

BSI, TT Club and TAPA EMEA have previously noted the growing number of thefts from facilities and, most notably, from trucks loaded with cargo and parked outside of facilities, since the beginning of the COVID-19 pandemic in 2020. In these incidents, employees of warehouses and facilities load cargo onto trucks before leaving them parked outside with minimal security overnight. When a truck driver arrives the next morning, they report that the cargo has been stolen.

Periodically throughout 2021 and 2020, areas near the Port of Calais in northern France experienced congestion due to changing rules and requirements for crossing the border to the United Kingdom. Migrants often waited along highways or rest areas and parking lots in the area hoping for an opportunity to stowaway onto the trucks waiting in these queues to cross the English Channel. In December 2021, regional authorities closed parking lots and rest areas in the Norkerque area of Calais due to this inherent risk.

Rising Shipping Costs and Congestion Driving Shortages Over New Cargo Theft Trends

Due to a reduction in shipping capacity, a premium on ocean freight, and long idle times at ports in the global north, African ports experienced a general reduction in ships making calls in 2021. Some countries, such as Namibia, Angola, Kenya, and Guinea, lost direct connections to foreign ports. These patterns of global trade, that favor countries in the global north, resulted in reductions to manufacturing capacity and shortages in some factories in African nations that depend on imports through the continent's ports.

Strict COVID-19 Containment Policies Disrupt Shipping in Asia

Strict COVID-19 restrictions contributed to reduced operational capacity in the shipping industry in 2021, especially in Hong Kong and China, where zero-COVID mitigation policies, including mandatory testing and lengthy quarantine periods, led to labor shortages that consequently increased the waiting times for ships awaiting port entry at ports in the Pearl River Delta. According to reports, an average of 13 ships per day awaited entry into Asian ports in December 2021. In January 2022, this number of ships increased to 22.5 per day.

As recently as March 2022, reports indicate that rising numbers of COVID-19 infections in Hong Kong, especially among truckers transiting between Hong Kong and mainland China, are significantly reducing local trucking capacity. Trucking capacity between Hong Kong and the mainland has reportedly experienced a 70 percent reduction. Hong Kong is reporting over 50,000 new cases per day, meaning that disruptions stemming from reduced trucking capacity are likely to continue through the beginning of the next quarter.



UNPACKING THE GLOBAL RISK OF INSIDER THEFT IN 2021 AND ONWARDS



Criminal organizations increasingly infiltrate supply chains or manage to bribe warehouse workers or truck drivers to steal cargo. Insider theft participation typically occurs when either warehouse or facility employees disclose confidential information pertaining to shipping and delivery times, or when employees intentionally leave doors and gates unlocked or ajar overnight, granting criminals easier access to carry out thefts. Another common tactic used during insider theft involves criminals bribing or coercing truck drivers to divert from their assigned delivery routes. During these route diversions, the truck operator will stop at facilities or designated locations along the road where criminals will unload partial loads of goods from the vehicle before the driver returns to their original delivery route.

Globally, the products most frequently involved in insider thefts in 2021 included agriculture (14 percent), food and beverage (12 percent), construction materials (10 percent), electronics (10 percent), and metal (nine percent). Notably, many of the materials used to produce these various goods, such as nitrogen, iron ore, lumber, steel, and semiconductors among others, have all experienced sharp price increases since the outbreak of the global pandemic.

Moreover, the price of crude oil has increased to levels not seen since 2009 and 2011, reaching about \$109 a barrel, at the time of this writing. This spike in the price of global crude oil has contributed to the increase in the overall cost to transport goods, as cargo trucks run on diesel fuel. The ongoing conflict between Ukraine and Russia is likely to exacerbate global fuel prices, especially if other countries follow the United States' decision to ban Russian oil imports.

A combination of general price hikes for goods, increasing costs to transport those goods, the ongoing threat from COVID-19 and the conflict in Ukraine will further disrupt global supply chains in 2022 and could create an environment more conducive to insider theft.

Identifying Global Areas of Concern for Insider Theft

According to BSI, TT Club and TAPA EMEA data collected throughout 2021, approximately 20 percent of all theft incidents reported in Europe involved some form of insider participation. Of these incidents involving insiders, approximately 56 percent occurred in warehouses, followed by 19 percent in production facilities. The top European countries of concern for thefts involving insider participation in 2021 were Russia and Italy; these thefts typically included elements of either supply chain corruption or organized crime.

The top countries of concern in Asia for insider theft in 2021 included India, Indonesia, China, Vietnam, and Bangladesh. In Asia, insider thefts accounted for 13 percent of all thefts in 2021. 37 percent of those insider theft incidents involved goods stolen from warehouses, and 18 percent of insider thefts involved goods stolen from production facilities.

Thefts involving insider participation are a growing concern in Bangladesh, where thefts along the Dhaka-Chittagong highway have significantly increased over the past year, according to several local reports and corroborated by BSI, TT Club and TAPA EMEA data. Members of highway robbery gangs are reportedly increasingly gaining employment as drivers for textile exporters to assist in the diversion and theft of goods that are en route to the Chittagong Port for exportation. In many cases, exporters do not become aware of the theft until they receive complaints from buyers detailing how some of the products were missing upon delivery.

In North America, reported incidents of insider-related theft in Mexico and the United States significantly outnumbered Canada. Roughly 5.2 percent of recorded theft incidents involved insider participation in North America in 2021. While this is relatively low when compared to Europe and Asia, the trend is on the increase from 2019 and 2020. In fact, since 2020, the risk of insider participation has increased by 48 percent, from 1.7 percent in 2020 to 5.2 percent in 2021, and the majority of the incidents are concentrated in Mexico and the United States.

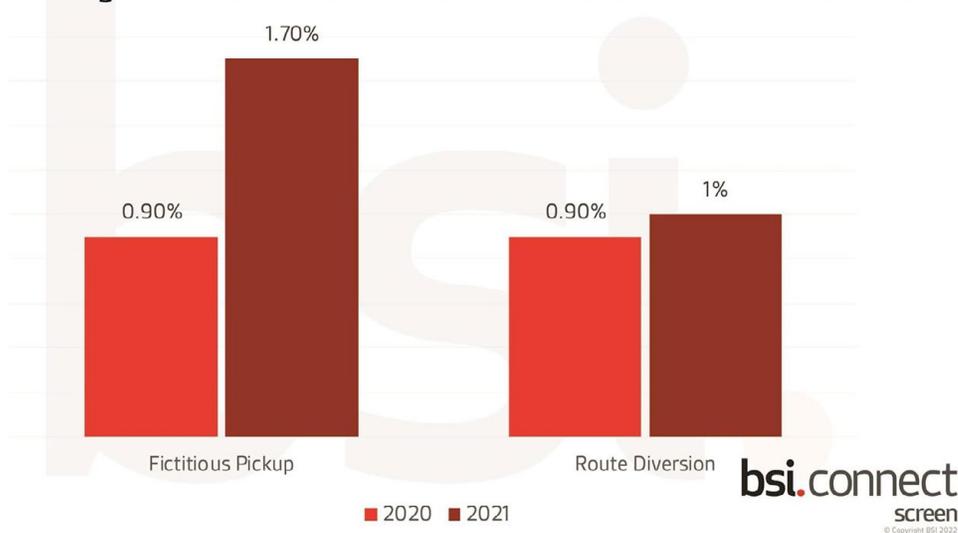
Historically, various countries in South America are susceptible to insider participation, including Brazil, Argentina, Colombia, and Peru. In South America, there was a slight increase in the risk of insider participation in recorded cargo theft incidents between 2020 and 2021, with the majority occurring in Brazil, Argentina, Peru, and Chile.

Industries at the greatest risk across both North and South America remain agriculture and prepared products, industrial and manufacturing, the pharmaceutical industry, petroleum and minerals, and consumer products and mass merchandising.

In the Middle East and Africa, evidence indicates that insider participation remained prevalent in 2021 and will likely linger in 2022 in the Gulf countries, especially the United Arab Emirates (UAE) and the Kingdom of Saudi Arabia (KSA). In these countries, criminals primarily target facilities to steal high-value products such as electronics. Despite government efforts to combat the issue, supply chain corruption remains a problem in the KSA and UAE, likely exacerbating trends of insider participation.

The KSA and UAE are also home to large free trade zones that form a structural part of the countries' economies. In these free trade zones, large volumes of cargo transit for import and re-export. This environment is conducive to smuggling schemes, while the large volume of trade coupled with supply chain corruption heightens cargo vulnerabilities. For instance, BSI has recorded incidents of security company employees in Saudi Arabia who reportedly conspired to steal from a vehicle in their charge, in addition to multiple instances in the United Arab Emirates of cargo thefts committed by employees and drivers.

Percentage of Thefts Conducted via Fraudulent Means 2021



Recommendations for Mitigating Risk of Insider Thefts

BSI, TT Club and TAPA EMEA recommend auditing cargo storage companies for stringent employee background checks and basic physical security measures, including CCTV surveillance. Installing GPS tracking on vehicles used in the transportation of goods will help in mitigating the potential for the diversion of goods along their delivery routes.

Threat awareness training, incentives for reporting security incidents, and ensuring that employees that leave the company have forfeited all property used to access facilities can also help mitigate the threat of insider theft.

Insider Participation Thefts a Growing Concern for Supply Chains in 2022

Cargo thefts involving insider participation continue to be a concern for global supply chains in 2022, especially with aggravating factors such as the global COVID-19 pandemic, rising cost of living, and the recent developments between Ukraine and Russia, which all have the potential to further exacerbate poor economic conditions, creating more incentives for insider corruption and cargo thefts generally.



CRIMINALS ADOPT NEW TACTICS TO TARGET THE CHANGING ENVIRONMENT FOR FREIGHT TRANSPORTATION

Criminals have adopted new tactics to target the changing environment for freight transportation. The growing reliance on technology and a rapidly changing market for sourcing materials and components have increased reliability and effectiveness, but also opened up new avenues of opportunity for criminals to take advantage of companies' increased vulnerabilities.

Some new tactics identified in the past year include the increased targeting of freight transportation service exchange apps and websites. These freight service applications, which have already been taken advantage of in recent years by criminals operating in South America and Brazil specifically, involve companies posting listings for truck drivers to respond to help move goods. By utilizing these applications that require significantly less vetting than other methods, criminals are more easily able to present themselves as legitimate carriers. Throughout 2021, transporters in Europe began reporting a rise in fictitious pickups and fraudulent carriers, highlighting the expansion of this risk worldwide.

Fraudulent Theft Top Locations Globally Include Brazil, Russia, Italy, and Mexico

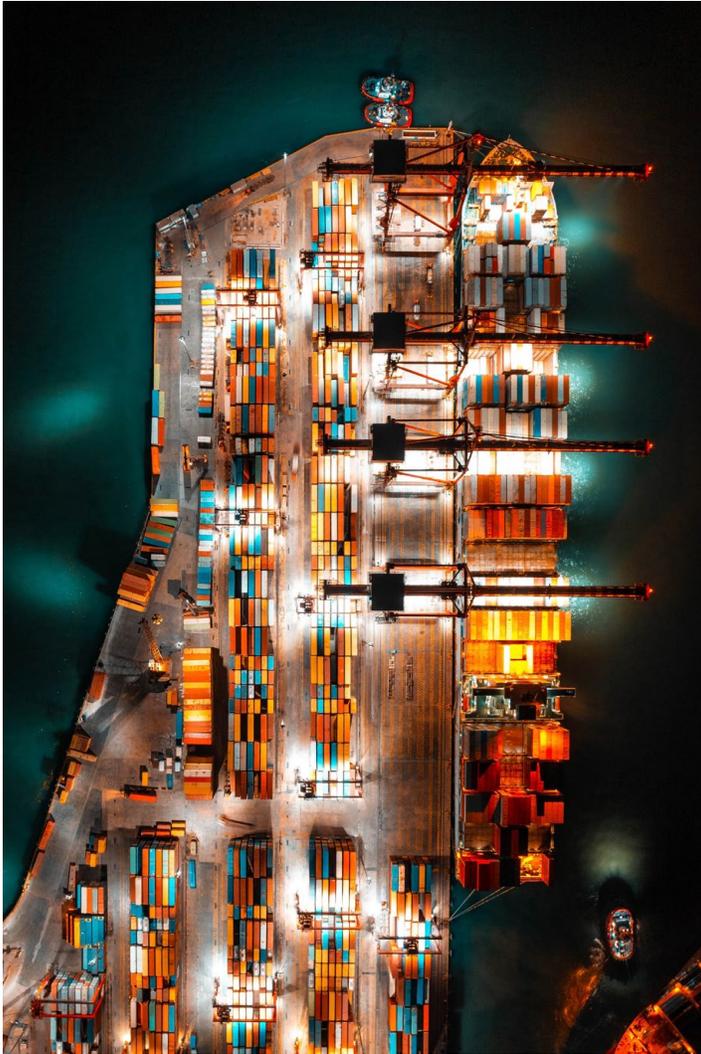
The top locations worldwide reporting fraudulent thefts, including route diversions and fictitious pickups, include Brazil, Russia, Italy, and Mexico. In such cases, thieves falsely present themselves as legitimate carriers, most often to steal food and beverage, and agricultural-type products. However, data from 2021 and 2022 so far appears to show a growing number of thefts of metals and construction supplies stolen via this method.

In Europe, thieves presenting themselves as legitimate carriers do not appear to target one specific commodity type over another; however, most products stolen generally follow global trends which show greater thefts of food and beverage, agriculture, automotive, and construction materials, as well as clothing and footwear, cosmetics and other high-demand consumer goods. While Russia showed over a four percent increase in the number of fraudulent thefts conducted, it is in Italy where the greatest percentage shift occurred. Although BSI, TT Club and TAPA EMEA did not record a single incident of fraudulent theft in Italy in 2020, in 2021 around ten percent of all fraudulent thefts globally occurred in Italy.

These thefts generally involve carriers picking up goods without arousing suspicion, and the theft often isn't even discovered until the legitimate delivery carrier arrives to pick up the goods. Oftentimes, this occurs when companies hire new or unknown transport companies and fail to conduct adequate due diligence checks before handing over goods. The subsequently diverted goods are often sent to eastern European countries for resale.

Thefts involving technology access do not always occur during pickups or at facilities. They often occur in transit or anywhere en route. In the United States, for example, our joint data noted that in the second half of 2021, criminals increasingly targeted pharmacies and products in unsecured parking lots. These types of thefts can vary in sophistication, with thieves going so far as to illegally access secure computer systems to steal identities and fraudulently represent themselves to unknowing companies. Reports worldwide also suggest that corrupt employees may inform criminals about shipment times and lanes, thus allowing them to target certain trucks and steal high-value goods.

The “rollover” theft tactic, prominent in the United Kingdom, involves thieves being aware of shipment times and locations for certain transportations to conduct thefts. They may obtain this information from corrupt employees or by managing to access technology regarding truck locations and utilization; and although companies generally have strict protocols in place for trucks departing their facilities, security may drop once the truck is in transit. In this tactic, thieves will even surround a moving truck with cars to allow one gang member to jump onto the truck to open the doors and throw the goods into the other cars. Oftentimes, such thefts are not realized until the delivery is made and items are recorded as missing.



Governments Modify Laws to Tackle These Evolved Threats

The issue of fraud conducted via freight exchanges and digital marketplaces has grown to the point where the French government has modified legislation to regulate these avenues through which companies and transporters can connect. Simultaneously, the United States has warned the Federal Trade Commission will track down companies that had not yet worked to resolve issues associated with cybersecurity risks, more specifically the Log4j vulnerability.

Known as the Mobility Orientation Law (LOM), the recent update to the French legislation reportedly goes beyond defining both marketplaces and participants by requiring those who are active on the platforms to verify their legitimacy through registration and communication requirements. The legislation now appears to hold participants, who engage in contractual services through these electronic marketplaces, responsible for a range of potential issues that could occur during the execution of the service, such as damage or loss of goods or the arrival of goods outside the designated timeframe. This legislation highlights how the focus is no longer only on the accessibility and usefulness of these types of online freight transportation service exchange sites, but also on the inherent risk that comes with communicating and

ultimately conducting business with parties via the internet.

The United States' government is also beginning to take a stronger stance on cybersecurity within the private sector. In August 2021, the Senate voted to dedicate over 1.9 billion U.S. dollars to growing cybersecurity defenses in the \$1 trillion infrastructure bill. These funds will be used to better secure critical infrastructure, provide money to a federal cyber office, and support organizations vulnerable to attacks. This funding included designating \$1 billion to help state and local governments deter attacks and protect data and information, \$100 million to increase the government's capabilities to respond to network attacks, and \$21 million to support the new National Cyber Director.

Furthermore, on December 14, cybersecurity experts announced the discovery of Log4j vulnerability in a registry library used by many U.S.-based companies. Experts referred to this vulnerability as “the most critical seen this year” and recommended updating systems immediately. On January 4, 2022, the Federal Trade Commission warned that it would track down companies that had not yet worked to resolve the Log4j vulnerability, thus holding businesses accountable for approving their cybersecurity.

Criminals in Russia Utilizing a Variety of Technologies to Conduct Thefts – Case Study

Cargo thefts in Russia frequently involve fraudulent means, both on the part of opportunistic employees and sophisticated, organized operations targeting high-value shipments.

In one incident, an individual registered a logistics company and completed multiple small-value cargo transport operations with third-party vehicles to build an appearance of credibility. Upon securing a multi-million transport operation for shampoo and lotion products, the individual instructed the third-party vehicle to deliver the goods to an incorrect location in an attempt to steal the shipment.

In another incident, experts warned that Russian-speaking criminal groups had expanded a scam to infiltrate online logistics platforms in Europe and the United States. The criminal groups operated the scam by advertising low-cost transportation services on logistics platforms. The thieves then moved the potential victim from the platform to a third-party messenger application to access bank card information, potentially utilizing stolen web pages from legitimate courier services. Sources report that there may be 40 such gangs conducting this scam, both within Russia and abroad in countries such as Romania, France, Poland, the United States, and multiple Central Asian republics.

Recommendations from BSI's Practice Director for Security and Resilience, Tony Pelli for mitigating these risks

To mitigate this risk, companies can take several actions, such as:

- Work to verify the trucking company - call the phone number they have listed, visit the website, and check to make sure the number they are using is not for a company that recently went out of business
- Where possible, set up pre-alerts - i.e. ask for the driver's name, trailer number, and license plate number in advance and have appointment times for each pickup
- Check driver IDs and record information about drivers - check to make sure their ID is not expired and matches the actual driver
- Train people in the dispatch/shipping office to recognize suspicious behavior - if the driver looks suspicious, shows up far too early, is wearing sunglasses/hoodie/etc. inside, something is probably wrong
- Make sure all carriers undertake employee background screening, including criminal history checks where possible
- Install cameras near dispatch/shipping/receiving windows to capture images of the driver's face for later ID if something goes wrong
- Take pictures/copies of IDs if that's allowed

ORGANIZATIONS HAVE BEEN FORCED TO ABRUPTLY ADAPT THE SUPPLY CHAIN SINCE THE START OF THE PANDEMIC

In recent years, many organizations have made drastic changes to their supply chain. Global events, such as the COVID-19 pandemic and truck driver shortages, have led organizations to utilize new workflow processes, in addition to new routes and transportation methods that differ strongly from what they had been doing routinely for years prior.

In many cases, organizations have not successfully completed proper due diligence before making these adjustments to secure their modified supply chains. In addition, staff shortages in a variety of industries have increased simultaneously, meaning many employees who are responsible for securing or transporting goods are operating without sufficient training, or suppliers are dependent on temporary staff members.

Changing Sourcing Locations Requires Thorough and Ongoing Risk Assessments

COVID-19 had an immense impact on organizations, requiring new business plans and workflow processes. These disruptions, in many cases, forced organizations to reassess the global distribution of their supply chains and where business partners and suppliers are located.

As a result, organizations are increasingly looking to shift supply chains to a more diversified model to mitigate potential risks and disruptions or potential non-compliance with new regulatory frameworks. As these considerations are made, it is important to conduct risk assessments for new sourcing locations to prepare for the different threats to the supply chain.

Assessing unique risks when entering a new location

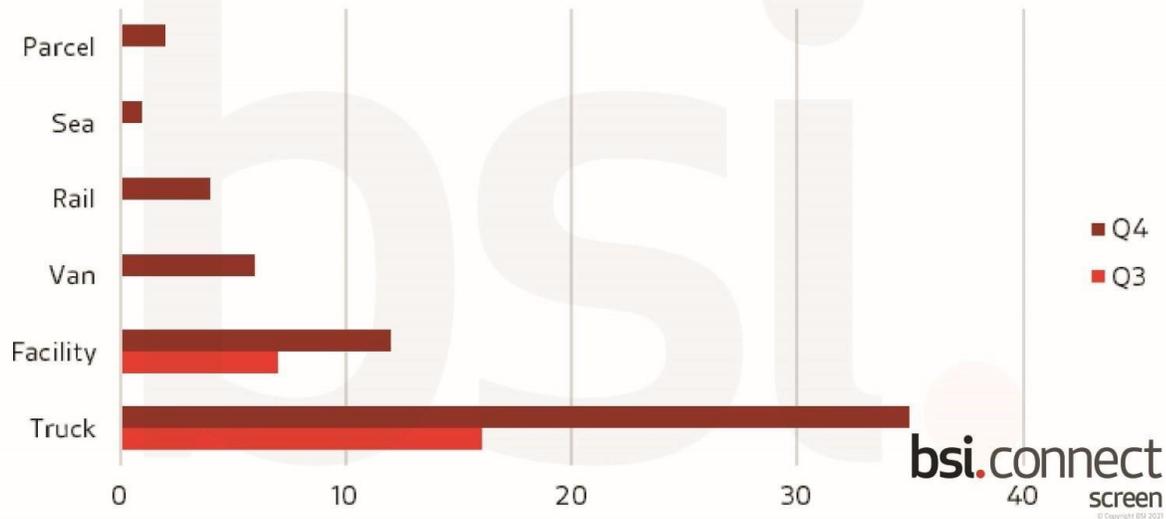
Assessing security risks should be a key component of any threat assessment. This should not stop solely at the level of crime affecting supply chains but also seek to determine the finer details of risks inherent to a given country. Each country has its own unique security environment, highlighting the importance of a robust risk assessment that considers all potential security, business continuity, sustainability, and regulatory threats associated with such a move.

In terms of security, the environment of cargo theft is a major component to consider when selecting a new location. For example, in Mexico, truck hijackings account for the most theft incidents in the country and thus pose the most significant risk of cargo theft. This security environment is different from those of other locations, such as many countries in Asia, where thieves tend to capitalize on poor access controls at facilities. This variation in theft tactics across geographic regions demonstrates that different protocols are necessary depending on the region: in Mexico, there should be a greater emphasis on securing shipments in transit, whereas in Asia, there should be a greater emphasis on securing shipments stored in facilities.

A similar approach applies to other security risks; while Asia does have illegal drug smuggling, the activity of cartels in Mexico is almost unparalleled and requires continued risk assessments. Mexican drug cartels felt the impact of the initial outbreak and spread of COVID-19 on their criminal supply chains. The measures to halt the spread of COVID-19 made it impossible to secure the chemicals needed to produce illegal drugs, along with the cocaine from South America that cartels sell both domestically and internationally. Perhaps most notably, the US-Mexico border being closed to all but essential traffic, namely freight, removed a key avenue for cartels to traffic illegal drugs into the United States. These factors combined had significant ramifications for supply chains as cartels increasingly looked to exploit corrupt individuals or to infiltrate supply chains deemed essential to replace this restricted transportation route. This shows how not just an initial risk assessment is key to a resilient supply chain, but also following up to remain current on shifting risks.

Increasingly, natural disasters and man-made disruption are also posing secondary or tertiary continuity challenges that often result in exposure to cargo theft. These incidents must be analyzed from multiple angles to determine the true potential impact on businesses.

Increase in Rail Thefts in the United States in Q4 2021



Risks related to ongoing and increasing truck driver shortages

In addition to risks relevant to geographic areas, organizations also face risks related to the ongoing truck driver shortage. Driver shortages cause operational and business impacts for many transport and logistics companies as they chase a diminished resource that is so critical for many industries. While there are industry initiatives to increase the number of drivers, these initiatives will take time to be established and return results.

In the meantime, organizations are turning to new and rapid hiring measures to maintain their business operations, potentially exposing the organization to additional risks. Thus, in this turbulent business environment, more than ever, organizations should apply and maintain appropriate and diligent personnel security measures and HR protocols when hiring new staff. These diligence measures will help to prevent the introduction of additional and unintended risk exposures.

Shifts in labor rights and environmental regulations

Two additional considerations for companies shifting supply chain operations to new locations are differing, and more recently increasing, regulations and the risk of labor rights and environmental violations. These two topics have recently become more intertwined than ever, with governments in North America and Europe requiring organizations to conduct due diligence and implement efforts to prevent human rights and environmental violations within their supplier networks. Companies choosing to relocate operations may fall under these new regulations.

The United States-Mexico-Canada (USMCA) trade agreement exemplifies this crossover of regulations governing business operations in both trade compliance and labor rights. Besides requiring all three countries to ban the entry of goods produced by forced labor, the USMCA also contains provisions aimed at improving the rights of workers in Mexico through labor union reforms. These reforms, and the potential penalties for non-compliant entities, can have detrimental impacts on the continuity of supply chains.

Although these outlined examples of risks may be daunting, organizations can take actions to mitigate the impact that these challenges can have on resilience. Conducting proper risk management can help to ensure that organizations remain resilient when shifting supply chain locations; however, this process is not without effort, as organizations must map out the supply chain, properly identify critical suppliers and routes, and keep abreast of knowledge around geographic risks in order to plan and best apply measures. Further, combining this knowledge with responses to questionnaires issued to suppliers can help an organization focus on potential risks in the supply chain and issue the proper corrective actions to reduce exposure to threats in new sourcing locations.



CASE STUDY: INCREASE IN RAIL THEFT DUE TO FACTORS SUCH AS PORT CONGESTION IS AN INCREASED WEAKNESS IN THE SUPPLY CHAIN THAT IS BEING EXPLOITED IN THE LOS ANGELES AREA

CASE: Rail Thefts Spike in the United States & Recommendations to Deter the Risk of Cargo Theft to the Rail Modality

In 2021, the supply chain had to cope with workforce shortages, blocked canals, and port congestion amid a pandemic that has fiscally weakened many companies. Due to the compounding factors, the twin ports of Long Beach and Los Angeles faced an unprecedented level of port congestion.

These ports are essential to U.S. supply chains as they handle about 40 percent of maritime imports into the United States, with most of the nearly 450 billion USD worth of goods moved through these ports eventually landing on a train in the area. Criminals have exploited the supply chain crisis to their advantage by preying on freight trains in East Los Angeles. At one point, Union Pacific reported thieves were breaking into an average of 90 containers a day in Los Angeles, with damages exceeding 5 million USD in 12 months.

BSI, TT Club and TAPA EMEA intelligence tracked and monitored similar spikes in rail theft in the United States, especially in Q4 2021 and carrying on into Q1 2022. In Q4, the rail modality accounted for 6.7 percent of recorded cargo theft incidents in the United States. While this is a significant jump from previous years, predominantly composed of either the facility or trucking modality, the majority of the thefts were limited to California, generally, and the East Los Angeles area, more specifically. However, Memphis, Tennessee is increasingly seeing an uptick in rail thefts as well, highlighting the shared risk factors that are conducive to higher rail thefts.

In California, multiple incidents in Q4 2021 indicated a rise in thieves targeting electronic products, along with apparel, and other high-value consumer goods. In one incident in late November, police reports indicated that thieves stole thousands of packages from moving freight train containers near Valley Boulevard and North Mission Road in Los Angeles, California. In these reports, the thieves utilized sharp tools to unhinge the container doors and loot the moving vehicle. In another incident on January 15th, 2022, 17 Union Pacific train cars were derailed in the same area where most thefts have occurred. The incident is still under investigation; however, Union Pacific is now considering diverting freight traffic away from LA County to reduce the risk of theft.

According to the Los Angeles Police Department (LAPD), Los Angeles County Sheriff's Department (LASD), and the California Highway Patrol (CHP), law enforcement has made roughly 100 arrests on these trains. As already stated, the rail operator Union Pacific identified attacks on up to 90 containers a day during the busiest shipping period

of the holiday season. To combat these threats, Union Pacific announced it has begun a drone surveillance system and implemented “specialized fencing and trespass-detection systems” in Los Angeles, California. Using these surveillance systems, Union Pacific has been able to make hundreds of arrests.

Similar to East Los Angeles, Memphis, Tennessee also experienced comparable spikes in rail thefts, not altogether surprising given that it is also among the most significant transportation and shipping cities in the country due to the number of Fortune 500 companies with distribution centers located in the area. Like East Los Angeles, it is especially at a higher risk because of its location, which is both in a lower socio-economic neighborhood with a history of high crime rates, as well as located near a secluded area of forest with a lower law enforcement presence. For example, in one incident in Q4 2021, 3 suspects broke into nine boxcars of a train and stole approximately \$500,000 worth of electronic goods at Mississippi Boulevard and Phelan Avenue in Memphis, Tennessee. In another incident, a mob, starting with 4 people and quickly escalating to 30 to 40 people, jumped onto a train and threw packages into the railway siding, robbing the freight car of its cargo.

Increases in rail thefts around Los Angeles and Memphis contributed to massive losses for companies relying on an already strained supply chain and has driven some major logistics companies to divert rail shipments away from essential rail services in Los Angeles County, for example.

Recommendations to mitigate the risks:

Tony Pelli, BSI's Practice Director of Security & Resilience shares recommendations for companies to counter the risk of rail thefts of containers:

- Seal rail containers with ISO 17712-compliant bolt or cable seals
- Consider the use of t-bar door locking devices to enhance container security
- Conduct checks on seals and door locking devices at all stops and document these checks
- Load freight as close as possible to the engine, locomotive, or front of the train
- Where possible, ensure that containers are loaded door-to-door on wagons or in the bottom of cars to prevent tampering with container doors
- Use GPS tracking on rail containers
- Consider using devices that can alert when container doors are opened
- Develop response protocols for security incidents and other irregularities
- Ensure that rail personnel are trained to inspect rail containers for irregularities
- Check that all rail yards used along the route are fenced, well-lit, patrolled by guards, and monitored by CCTV, with controlled access to the yard

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'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 INSURED, SERVING THE INDUSTRY.



Michael Yarwood
Managing Director, Loss Prevention

T: +44 (0) 20 7204 2653
M: +44 (0) 7788 873935
E: michael.yarwood@thomasmiller.com



Peregrine Storrs-Fox
Risk Management Director

T: +44 (0)20 7204 2254
M: +44 (0)7880 786909
E: peregrine.storrs-fox@thomasmiller.com



Laurence Jones
Risk Assessment Director

T: +61 2(02) 8262 5800
M: +61 413 011 791
E: laurence.jones@thomasmiller.com

REDUCING THE RISK OF CARGO LOSSES

The Transported Asset Protection Association (TAPA) was founded in 1997 by Manufacturers and Logistics Service Providers with a mission to minimise losses from their supply chains resulting from cargo thefts.

Today, in the Europe, Middle East & Africa (EMEA) region, TAPA EMEA has a record and growing membership of over 750 companies, now also including Insurers, Law Enforcement Agencies and Security Service Providers.

The cost of cargo crime is a major concern for all supply chain stakeholders and can have a detrimental effect for consumers too in terms of delayed orders, product shortages and higher prices. A European Parliament study has previously identified that cargo crime in Europe alone costs businesses more than €8.2 billion per annum, while research by TAPA EMEA in Germany, in partnership with other industry associations, identified national losses and damages exceeding €2.2 billion a year from an estimated 26,000 attacks on trucks annually. TAPA EMEA's 'by the industry, for the industry' supply chain resilience and cargo security solutions include industry Standards and cargo crime incident intelligence:

Security Standards

TAPA EMEA offers three industry Standards and certification programmes, which are reviewed and updated by its supply chain security members every three years to ensure they are as efficient as possible and fit-for-purpose to provide protection against current and emerging risks. The Standards are:

- Facility Security Requirements (FSR)
- Trucking Security requirements (TSR)
- Parking Security Requirements (PSR)

These are minimum security Standards and are respected as the most effective industry Standards for supply chain security. Further information can be found on the TAPA EMEA website. TAPA EMEA security Standards are now a requirement in many logistics contracts.

Incident Intelligence

The TAPA EMEA Intelligence System (TIS), launched in 2022, is the Association's most advanced data and analysis tool to help combat cargo losses.

Via the TIS dashboard, members can quickly search for current and historic cargo crime incident data, using mapping and routing tools to filter data by a wide variety of topics, including searches for:

- Type of incident
- Location of incident
- Modus operandi
- Value of stolen products
- Products target
- Region
- Country

TIS also integrates information which allows our Manufacturer and Logistics Service Providers to see facilities and trucking operators which have TAPA EMEA Facility Security Requirements (FSR) and Trucking Security Requirements (TSR) supply chain security certifications. They can also search TAPA EMEA'S growing database of secure truck parking locations across the region and identity parking place operators supporting the Parking Security Requirements (PSR) Standard.

Networking and Communication

TAA EMEA also delivers insight and analysis for its members through its annual Face-to-Face and Virtual conferences, twice-monthly intelligence sharing webinars, a monthly digital magazine and incident alerts.

Contact Us

To find out more about TAPA EMEA, the Association's security Standards or how to share cargo theft intelligence, please contact info@tapaemea.org or visit www.tapaemea.org



TAPA EMEA
Thorsten Neumann
President & CEO
E: Thorsten.Neumann@tapaemea.org



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 Global Intelligence Analysts



Anna Lee Robbins
Anna.Robbins@bsigroup.com



Jason Willoughby
Jason.Willoughby@bsigroup.com



Erica Bressner
Erica.Bressner@bsigroup.com



Marianna McMillan
Marianna.McMillan@bsigroup.com

bsi.connect
screen

4150 Drinkwater Blvd. Ste 160, Scottsdale, AZ 85251
supplychain@bsigroup.com | bsigroup.com/supplychain

