



Allianz Commercial

Cargo theft: What's driving it and how to mitigate the risks

There has been a significant rise in cargo theft in recent years, with a change in the goods being targeted and increasingly sophisticated tactics used by criminals. Businesses need to be aware of the heightened risk and review their logistics and supply chain strategies to mitigate it.

Figures and trends

- Supply chains in North America faced a spike of 13% in the volume of cargo theft between 2021 and 2022, with an increase in value of 16%¹, a trend that has continued in 2023.
- While electronic goods remain highly vulnerable, thieves are increasingly targeting household items and food and beverage, indicating that inflationary pressures are driving changes in criminal activity.
- In line with evolving supply chains, criminals are developing sophisticated and organized methods to gain access to cargo, ranging from straightforward theft, cyber-attacks, fraud, and technology-based crime.
- The consequences for businesses can be grave. Supply chain disruptions caused by theft prevent shippers delivering products to customers promptly and safely, while a failure to meet contractual obligations can lead to reputational risk and loss of market share.
- With a stolen commodity value of \$107mn in 2022 – a significant increase on the \$68mn reported in 2020² – cargo theft is clearly a risk that calls for heightened vigilance.
- Similarly, Allianz has seen an uptick in cargo theft incidents in recent years and particularly in transportation and logistics. In North America, the number of theft claims has increased for the past six years in a row in this area with a 20% increase year-on-year in 2022 (169 claims). The total for 2023 is likely to surpass 2022.

1. CargoNet, Supply Chain Risk Trends 2020-2022

2. CargoNet, Supply Chain Risk Trends 2020-2022

The top five goods most in demand

Household items (e.g. appliances and furniture), electronics and food and beverage top thieves' target lists

Commodity	Number of incidents
Household items	210
Electronics	206
Food and beverage	197
Building materials	65
Apparel and accessories	57

Cargo theft incidents North America, 2022. Source: CargoNet



When and where is theft occurring?

Warehouses and distribution centers are the most vulnerable locations across North America, with 407 reported incidents, followed by parking lots (322), and truck stops (248)³.

Incidences of cargo theft in North America vary according to state, with areas that are ports of entry and also large distribution centers dominating. The hotspot for cargo theft in 2022 was California, with 445 reported cases, over a third of them concerning electronics (36%), followed by household goods (21%). Texas was the second most afflicted state, with 228 cases, nearly a quarter (23%) concerning food and beverage, while Florida reported 161 cases of cargo theft, with food and beverage and household goods (both 22%) the leading theft objects⁴.

Most theft takes place on Fridays (19% of cases in 2020, 17% in 2021 and 18% in 2022), with Saturday and Sunday showing the lowest occurrence of cargo theft (around 11% of cases per year between 2020 and 2022)⁵. While there is no definitive answer to why this is the case, many drivers take their cargo to their homes or lots for the weekend to commence transport early on Sunday or Monday. When trucks are outside safeguarded distribution centers this makes their cargos easier to steal.

The different types of cargo theft

Criminals use a variety of tactics when targeting and stealing cargo⁶. Straight theft (where the driver and/or commodity is being watched by thieves) was the most common occurrence of cargo theft in North America in 2022, with 1,059 reported cases, compared to 316 cases of burglary and theft (more opportunity-driven), 139 cases of fictitious pick-up (where a criminal uses false ID or documentation to impersonate a carrier), and 92 cases of broken seal⁷.

Straight cargo theft

Products are stolen from their storage site, typically truck stops, warehouses or distribution centers, train stops, and loading and unloading docks. Sometimes thieves target commodities by staying near a warehouse and waiting for the cargo to be loaded on to the trailer. They follow the trailer until the driver makes a stop to rest or spend the night. The thieves then break the seal and take the entire cargo or a few targeted items.



3. CargoNet, Supply Chain Risk Trends 2020-2022

4. CargoNet, Supply Chain Risk Trends 2020-2022

5. CargoNet, Supply Chain Risk Trends 2020-2022

6. LVT, Cargo Theft Trends: A Bomb to the Bottom Line, February 6, 2023

7. CargoNet, Supply Chain Risk Trends 2020-2022

Strategic or deceptive cargo theft

Criminals disguise themselves as legitimate drivers, employees or business representatives and deceive truck shippers, brokers, and carriers. This type of theft can include identity theft and fictitious pick-ups.

For example, in recent months, Allianz has seen claims where the motor carrier is holding the cargo hostage and will not release and/or deliver the cargo until they are paid for the transit. They proceed to open the seal, transload and store the cargo in a warehouse until payment has been received.

Another method criminals employ is to illegally access motor carrier information, which contains load details. They then contract another company (rate confirmation and bill of lading has already been issued) to have a driver pick up the cargo and take it to another location. They check the load for GPS signals placed by the shipper for tracking purposes, and finally hire another company to move the load from the warehouse to other locations.

Technology-based cargo theft

Criminals sometimes use devices that detect hidden GPS trackers placed in or on the cargo. These devices interfere with the signals of GPS trackers and make it more difficult to recover stolen goods. Usually, the driver is not involved but the thieves conduct countersurveillance and put GPS trackers on to the units. Once the driver goes to sleep, they remove the cargo from the trailer. Thieves have also been known to use AirTags (small tracking devices), staying close enough to the driver and cell reception to get a signal.

Another tactic is to use a device called a cellphone 'jammer', which are illegal to use in many jurisdictions. The jammer blocks all signals (GPS and cellphone up to 40ft-60ft), meaning cargo cannot be tracked once it is stolen.

Cyber crime

Thieves exploit cyber weaknesses to gain access to computer systems and goods, using tactics such as phishing emails, when they impersonate a trusted supplier or entity. Criminals also use emails to install malicious programs that grant hackers access to valuable data from a company's system. The information can then be used to forge invoices and delivery documentation or to divert shipments.



Cargo theft case studies

Allianz has already seen many of the trends above playing out in the claims environment.

One prime example is an occurrence in which pallets of electronics arrived with extensive shortages at their destination. An investigation revealed that not all products from the containers had been loaded onto the trailers destined for the customer. A police investigation found there had been a theft by an organized group using pseudonyms to secure load numbers and fraudulently pick up shipments. The criminals had pretended to be subcontractors of the designated carrier, picking up the freight and sealing the trailer, but never delivered it to the destination.

Another scheme involved the identity of motor carriers being changed without their consent or knowledge by criminals. The freight brokers assigned loads for transport to what they thought was the legitimate motor carrier as business-as-usual, making contact and issuing a rate confirmation. The freight broker was later notified by the client that the cargo did not arrive. When they contacted the legitimate motor carrier, they said they were never given nor accepted a load for transport from the freight broker.





Risk management and mitigation

It is essential for any company at risk of cargo theft to identify, manage and mitigate security threats using internal processes and external advice where necessary. Here is a checklist for building resilience into your operations and keeping your goods and staff safe.

Run a tight warehouse

A well-run warehouse and transportation operation is the first step towards tackling security hazards. This should include stringent security processes and procedures, security and loss prevention training and awareness programs, and robust hiring practices for employees as well as third-party partners.

Reduce the chance of a fraudulent pick-up by controlling access to key information and keeping drop-off locations as confidential as possible.

Carry out internal and external security audits to determine where the strengths and vulnerabilities lie in your security practices.

Secure facilities

Cargo warehouses and storage facilities should be equipped with the appropriate security measures such as access control systems, surveillance cameras, monitor surveillance systems, including perimeter security, alarms and sensors. Ensure the exterior and surrounding areas are well lit.

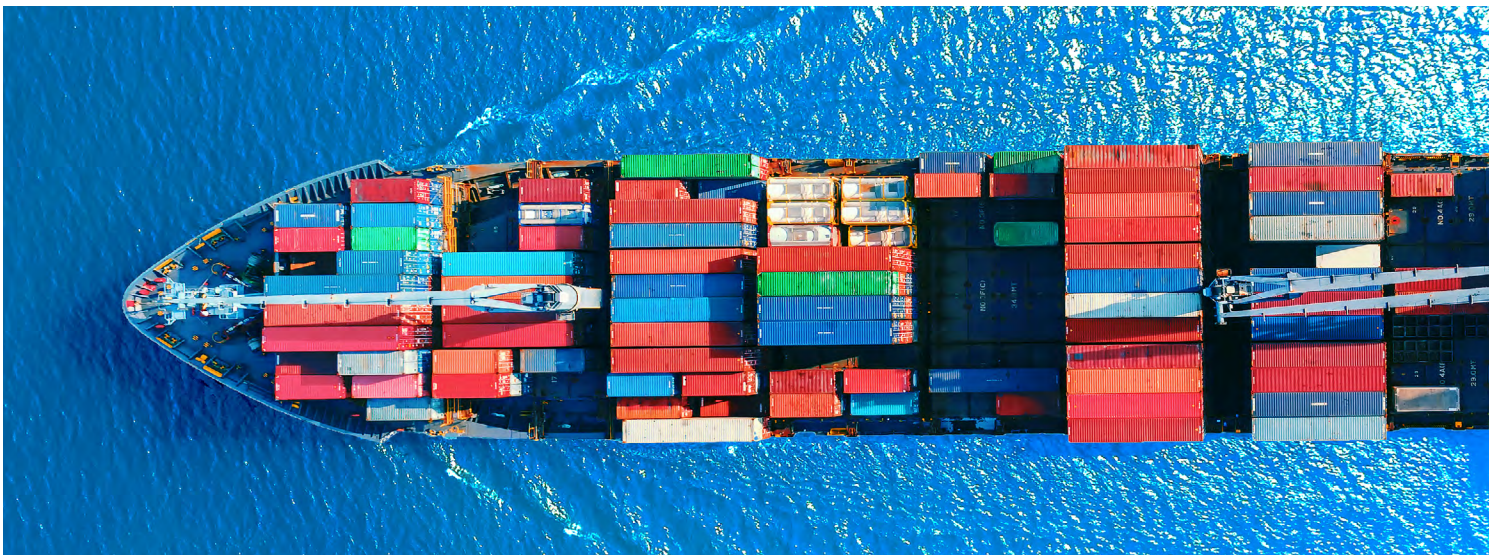
Work together with other companies, industry experts, trade associations, law enforcement agencies, and security professionals to stay abreast of best practices and emerging trends in cargo theft deterrence.

Technology and security devices

Surveillance technology can be effective in preventing cargo theft or identifying criminals if a cargo gets stolen. Some devices include front-side and rear-facing cameras on trucks, tracking devices (GPS and/or Radio Frequency Identification (RFID)), and high-security seals and locks, including landing gear locks, kingpin locks, air-cuff locks, and truck immobilizers.

Transit security measures

Educate your drivers in how to recognize potential threats or suspicious activities and empower them to take preventive action. Maintain frequent communication between the driver and the dispatcher and encourage drivers to report security concerns immediately. Route plans should consider hot spots and hot times and minimize wait time. Aim to keep cargos moving, avoid leaving loaded trailers unattended, park them in secured locations wherever possible, and use geofencing tracker apps, which create a virtual perimeter of a location, alerting you when the device enters or leaves the area.



For help and information

The Transported Asset Protection Association (TAPA) is an organization whose mission is to assist in tackling the multibillion-dollar cargo theft problem in supply chains globally. It achieves this through the development and application of global security standards for trucking services and for warehousing and storage facilities. For more information on TAPA services and insights into effective loss prevention, visit the [website](#).

Allianz Risk Consulting (ARC) has been a member of TAPA since its inception. ARC Marine specifically is a multidisciplinary team of risk engineers who provide clients with tailormade solutions and proactive risk management for cargo theft prevention depending on their business case model, commodity, location, and mode of transportation.

Risk Consulting

Rahul Khanna

Global Head of Marine Risk Consulting

rahul.khanna@agcs.allianz.com

+ 1 929 638 6655

Randall Lund

Senior Marine Risk Consultant

randall.lund@agcs.allianz.com

+ 1 808 927 5994

Damon Finneran

Senior Marine Risk Consultant

damon.finneran@agcs.allianz.com

+1 401 527 5049

Claims

Florian Krampitz

Director of Marine Claims, North America

florian.krampitz@agcs.allianz.com

+1 312 859 1318

Erika Cordova-Cabrera

Claims Specialist, Marine

erika.cordova-cabrera@agcs.allianz.com

+1 312 937 0804

Rebecca Overton

Director, Inland Marine Claims

rebecca.overton@agcs.allianz.com

+1 713 599 1174

Copyright © 2023 Allianz Commercial / Allianz Global Corporate & Specialty SE. All rights reserved.

The material contained in this publication is designed to provide general information only. While every effort has been made to ensure that the information provided is accurate, this information is provided without any representation or guarantee or warranty of any kind about its accuracy and completeness and neither Allianz Global Corporate & Specialty SE, nor any other company of Allianz Group can be held responsible for any errors or omissions. This publication has been made on the sole initiative of Allianz Global Corporate & Specialty SE.

All descriptions of services remain subject to the terms and conditions of the service contract, if any. Any risk management duties as laid down in the risk service and/or consulting contracts and/or insurance contracts, if any, cannot be delegated neither by this document, nor in any other type or form. Some of the information contained herein may be time sensitive. Thus, you should consult the most recent referenced material. Some of the information given in this publication may not apply to your individual circumstances. Information relating to risk services is intended as a general description of certain types of risk and services to qualified customers. Allianz Global Corporate & Specialty SE do not assume any liability of any kind whatsoever, resulting from the use, or reliance upon any information, material or procedure contained in this publication. Any references to third party websites are provided solely as a convenience to you and not as an endorsement by Allianz Global Corporate & Specialty SE of the content of such third-party websites. Allianz Global Corporate & Specialty SE is not responsible for the content of such third-party sites and does not make any representations regarding the content or accuracy of materials on such third-party websites. If you decide to access third-party websites, you do so at your own risk.

Allianz Global Corporate & Specialty SE
Dieselstr. 8, 85774 Unterfoehring, Munich, Germany

Images: www.shutterstock.com

August 2023