

Marine Risk Engineering

Strengthening cargo security
in our stretched supply chain





Global Supply Chain Challenges

Today's supply chain has developed into an efficient system allowing for the rapid flow of good across the world. With growing global consumption, significant challenges continue to bring risk into the supply chain, including cyber insecurity and cargo theft. In fact, cargo theft reached an all-time high in 2024, with a global cost of an estimated \$35 billion.¹

Record container volume, consumer demand and a labor shortage are just some of the factors contributing to this trend. Cargo security remains a driver of supply chain continuity but is being challenged by an increase in opportunistic thieves exploiting the current conditions and targeted efforts for high-demand products.

Increased Cargo Security Risks

Over the course of 2024, the ports in North America in terms of total cargo volume, indicated a 13% growth over the previous year.² While this growth may be impacted by tariffs and other aspects of uncertainty, there are indicators that global transport will continue to increase over time.

Photos and media headlines have made it clear of the severe challenges the industry often faces. Yet, the record volume of imports is having varying effects on numerous port infrastructures. In terms of infrastructure, lagging services critical to domestic and port operations to move cargo containers at the same rate of discharge from vessels appear to be presenting challenges.

One indicated cause of this is attributed to a shortage of available drivers. Data suggests a short fall of between 24,000³ and 60,000⁴ drivers, which not only slows cargo movement but costs an estimated \$95.5 million weekly.³

A recent dockworkers strike, which was initiated to strengthen terms related to wages and automation concerns, demonstrated the complex challenges of navigating a global supply chain.⁵ Unfortunately, cargo owners also need to factor risks well beyond the port gates. CargoNet, which tracks supply chain thefts, reported record theft in 2024, with "3,625 reported incidents" at an average cost of \$202,364 per theft.⁶ Cargo thieves are exploiting the backlog and placing more strain on an already struggling supply chain.

In 2024, there were **3,625** theft incidents reported, which represents an increase of **13%** over the previous year.²

The top targeted locations for cargo theft in 2024 were **Warehouses or Distribution Centers** and **Truck Stops.**⁶



Another common issue is fictitious pickups and fraudulent events where criminals either make up or steal a legitimate carrier's identity and solicit freight as authorized business with no intention of delivering.

Cargo theft is always a threat to the supply chain and during challenging times, it is important for businesses to remain vigilant as the industry faces complex and sometimes precarious conditions. Whether thieves gain intel from inside sources for high-demand products or seek out unmonitored 'soft targets', shippers and logistics service providers should continue to review their security standards to better prevent losses.



Cybersecurity as a Hedge Against Risk

Technology has revolutionized logistics, enhancing efficiency and meeting the demands of a global consumer base. This technological advancement, however, also exposes shippers and manufacturers to significant vulnerabilities, which can result in the loss of massive amounts of cargo each year. Threat actors are increasingly able to exploit security vulnerabilities and access critical data, identifying the precise route or location of valuable shipments. This enables them to steal cargo directly from ports, rail yards and airports, putting businesses and the global supply chain at risk.

Cargo thieves utilize sophisticated tactics to manipulate victims and reroute freight, exploiting opportunities to access sensitive information often stored in unsecured software, electronic load documents or email correspondence. As is the case across the board, phishing and stolen credentials are the most common methods used to access private, business-critical information used in targeting cargo. What is even more alarming, per a report from Transport Topics, is that 21% of incidents involve organizational insiders, including current or terminated employees, seeking to exploit and profit from their positions.⁷ They are often able to access unsecured computers and print extra copies or take photos of sensitive information, compromising business operations.

Singular cyber incidents can also create devastation. For instance, when Maersk was impacted via the NotPetya cyberattack, the company's operations were shut down, including and its "container ships carrying tens of millions of tons of cargo, representing close to a fifth of the entire world's shipping capacity, was dead in the water".⁸ NotPetya, which utilized open-source software and targeted known vulnerabilities, allowed for fast-paced and automatic replication of the virus that shut down entire networks across the world. Entire industries were inoperable, some lasting for several days. The total damage of the NotPetya cyberattack has been estimated at \$10 billion, with Maersk losing several hundred million dollars.

As cyber incidents become more prevalent, it is imperative for organizations to maintain a strong cybersecurity program. Engaging in regular risk assessments can help organizations uncover and remediate vulnerabilities that may lead to a debilitating attack before any damage is done. This could include employee training to limit phishing and social engineering attacks and developing a well-practiced incident response plan, so team members are prepared in the event an incident occurs.



General process continuity and improvement factors to consider

- Expand screening of new and temporary employees to avert inside information leaks relative to operations and security procedures
- Mitigate fictitious pick-up with expanded truck and driver verification before releasing a load
- Carefully record all details of truck, trailer and driver credentials where necessary (tags, color, unique markings, etc.) before the driver arrives for pick-up
- Escalate review of any known vessel port diversions and steamship line appointed motor transit
- Local drayage that becomes a long haul due to port diversions should include a review of driver and equipment qualification
- Elimination of truck brokering, and if unavoidable, required notification to verify the carrier and driver are legitimate
- Control truck driver behavior as it relates to layovers, stops and transit routes
- Prepare a “layered” approach to security
 - Procedural (controlling actions by employees, visitors and logistics service providers)
 - Know where your freight is: Electronic freight tracking, periodic updates and escalation when protocols are not followed in transit (GPS tracking installed on truck and or trailer) or preferably covert (embedded in cargo)
 - Installation of locking mechanism in addition to metal or bolt seals
- Regular cybersecurity Risk Assessments

Striking a practical balance of delivering products as quickly as possible while bolstering security and becoming a hard target is not a singular effort. A layered security approach hardens potential targeting of goods. When successful, the intent of thieves tends to move on and focus upon less protected cargo. It should be an organizational goal amongst all stakeholders in the process while cargo is in their care, custody and control. Please consider industry associations and insurers for support to build out these programs. It is a collaborative effort yet again to ensure the interruption consumers and the economy are experiencing is not exacerbated by bad actors taking advantage of this situation.



The 2021 **stranding of massive container ship**, the Ever Given, in the Suez Canal, cost organizations

\$9.6 billion per day.⁹

Various **port and dockworkers strikes** in 2024 cost the U.S. economy approximately

\$4.5 billion per day.¹⁰

Organizations cannot afford to have maritime transports delayed by **labor strikes** at ports or **supply chain insecurity and interruption**.

To learn more about *cargo security* or how ZRS can help with your Marine Risk Engineering needs, contact us:



800-982-5964



risk.engineering@zurichna.com



us.zurichresilience.com



Sources

1. Souza, Kim. "The Supply Side: Cargo Theft to Rise 25% in 2025; \$35 Billion Lost in Supply Chain." *Talk Business & Politics*, 2 Apr. 2025.
2. CBRE. *Annual North American Cargo Volume Increases by 13%*. CBRE, 26 Feb. 2025.
3. De Leon, Pamela. "Truck Driver Shortage Costs Freight Industry \$95.5 Million Weekly." *Commercial Carrier Journal*, Feb. 2025.
4. McCareins, Michael. "Is There a Truck Driver Shortage in 2025?" *altLINE*, 9 Apr. 2025.
5. Bonamo, Mark J. "US dockworkers strike over wages and automation in fight that could lead to shortages." *New Jersey Monitor*, 1 Oct. 2024.
6. Verisk. "2024 Supply Chain Risk Trends Analysis." *Cargonet.com*, 21 Jan. 2025.
7. Transport Topics. *2022 Cargo Theft Report*. TT CLUB, TAPA EMEA and BSI Connect SCREEN Intelligence, 1299 Zurich Way, Schaumburg, IL 60196, USA. The opinions expressed herein are those of Zurich Resilience Solutions as of the date of the release and are subject to change without notice. This document has been produced solely for informational purposes. All information contained in this document has been compiled and obtained from sources believed to be reliable and credible but no representation or warranty, express or implied, is made by Zurich Insurance Company Ltd or any of its affiliated companies (Zurich Insurance Group) as to their accuracy or completeness. This document is not intended to be legal, underwriting, financial, investment or any other type of professional advice. Zurich Insurance Group disclaims any and all liability whatsoever resulting from the use of or reliance upon this document. Nothing express or implied in this document is intended to create legal relations between the reader and any member of Zurich Insurance Group. Certain statements in this document are forward-looking statements, including, but not limited to, statements that are predictions of or indicate future events, trends, plans, developments or objectives. Undue reliance should not be placed on such statements because, by their nature, they are subject to known and unknown risks and uncertainties and can be affected by numerous unforeseeable factors. The subject matter of this document is also not tied to any specific service offering or an insurance product nor will it ensure coverage under any insurance policy. No member of Zurich Insurance Group accepts any liability for any loss arising from the use or distribution of this document. This document does not constitute an offer or an invitation for the sale or purchase of securities in any jurisdiction.
8. Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired*.
9. Russon, Mary-Ann. "The cost of the Suez Canal blockage." *BBC News*, 29 March 2021.
10. Krisher, Tom, Vejjongsa, Tassanee, and The Associated Press. "U.S. economy could lose \$4.5 billion a day as ports hit with biggest dockworkers strike since 1977." *Fortune*, 1 Oct. 2024.



Contact us:



800-982-5964

risk.engineering@zurichna.com

us.zurichresilience.com

Zurich Resilience Solutions

1299 Zurich Way, Schaumburg, IL 60196-1056

This is a general description of services such as risk engineering or risk management services provided by Zurich Resilience Solutions, which is part of the Commercial Insurance business of Zurich Insurance Group and does not represent or alter any insurance policy or service agreement. Such services are provided to qualified customers by affiliates of Zurich Insurance Company Ltd, including but not limited to Zurich American Insurance Company, 1299 Zurich Way, Schaumburg, IL 60196, USA, and The Zurich Services Corporation, 1299 Zurich Way, Schaumburg, IL 60196, USA. The opinions expressed herein are those of Zurich Resilience Solutions as of the date of the release and are subject to change without notice. This document has been produced solely for informational purposes. All information contained in this document has been compiled and obtained from sources believed to be reliable and credible but no representation or warranty, express or implied, is made by Zurich Insurance Company Ltd or any of its affiliated companies (Zurich Insurance Group) as to their accuracy or completeness. This document is not intended to be legal, underwriting, financial, investment or any other type of professional advice. Zurich Insurance Group disclaims any and all liability whatsoever resulting from the use of or reliance upon this document. Nothing express or implied in this document is intended to create legal relations between the reader and any member of Zurich Insurance Group. Certain statements in this document are forward-looking statements, including, but not limited to, statements that are predictions of or indicate future events, trends, plans, developments or objectives. Undue reliance should not be placed on such statements because, by their nature, they are subject to known and unknown risks and uncertainties and can be affected by numerous unforeseeable factors. The subject matter of this document is also not tied to any specific service offering or an insurance product nor will it ensure coverage under any insurance policy. No member of Zurich Insurance Group accepts any liability for any loss arising from the use or distribution of this document. This document does not constitute an offer or an invitation for the sale or purchase of securities in any jurisdiction.

In the United States, risk engineering and risk management services are provided by The Zurich Services Corporation.

©2025 The Zurich Services Corporation. All rights reserved.

A1-P1004446-A (05/25) P1004446

