



TAPA APAC INTELLIGENCE SYSTEM

TIS Annual Report 2024

Driving Supply Chain Resilience Against Cargo Crime



TRANSPORTED ASSET PROTECTION ASSOCIATION ASIA PACIFIC

WWW.TAPA-APAC.ORG/TIS

Foreword

The Transported Asset Protection Association Asia Pacific (TAPA APAC) Intelligence System (TIS) Annual Report 2024 aims to provide insights on the evolving trends and challenges surrounding cargo crime, offering stakeholders a perspective on the state of supply chain security in Asia Pacific using the verified and authenticated TIS data collected for the year of 2024.

TAPA is the leading global association that unites supply chain industry leaders and organizations with the common aim of upholding the highest standards of supply chain resilience and sustainability. In Asia Pacific, TAPA APAC helps manufacturers/shippers and logistics service providers to minimize cargo theft losses and increase the resilience of their supply chains through its Standards certification, training and membership programmes.

TAPA APAC TIS is a tool which enhances the security and resilience of members' supply chains by providing insights into recorded incidents and cargo crimes globally, as well as information on facilities and trucking operators which meet the TAPA Standards Certifications.

The TIS database of cargo crime are gathered by TAPA members' first-hand reporting, professional intelligence consultancy, insurers, Law Enforcement Agencies, and open media sources. TAPA TIS dedicated team scrutinize and verify all information to confirm its legitimacy, assuring that only valid and substantiated incidents are acted upon, thereby upholding the highest standards of security and reliability of all TIS information.

This report has been prepared by the TAPA APAC TIS team to the best of knowledge and interpretation based on the verified 2024 TIS data. The contents of this report are made available for informational purposes only. Neither TAPA APAC nor its advisors shall be liable for losses that arise in any way due to the reliance on the contents contained in this report.

[READ MORE ABOUT TIS >](#)

[TIS ANNUAL REPORT 2023 >](#)

Contents

Global Cargo Crime Overview

Supply Chain Losses Across the Globe

04

Global Cargo Crime Trends

Cargo Crime Insights by Type

05

Largest Single Incident in Asia Pacific

Six Arrested in USD 4.2M Laptop Heist at Chennai Port

06

Asia Pacific Per Quarter Analysis

Comparing 2024 and 2023 Data by Quarter

07

Asia Pacific Cargo Crime Trends

A concise overview examining cargo crime by country, incident categories, modus operandi, location types, and product categories

08

Internal Employee Involvement Case

Sydney Employee Charged for Theft of 8,000 Solar Panels Worth USD 780,000

10

A TIS Case Study

Improving Cargo Security Practices in High-Risk Shipments

13

Join the 2025 TIS Working Group

2025 TIS Working Group is Recruiting Its Members

16

Combatting Cargo Crime with TAPA APAC

Insights from TAPA APAC

17

2024 Statistical Full Breakdown

A detailed breakdown of all recorded cargo crime for 2024

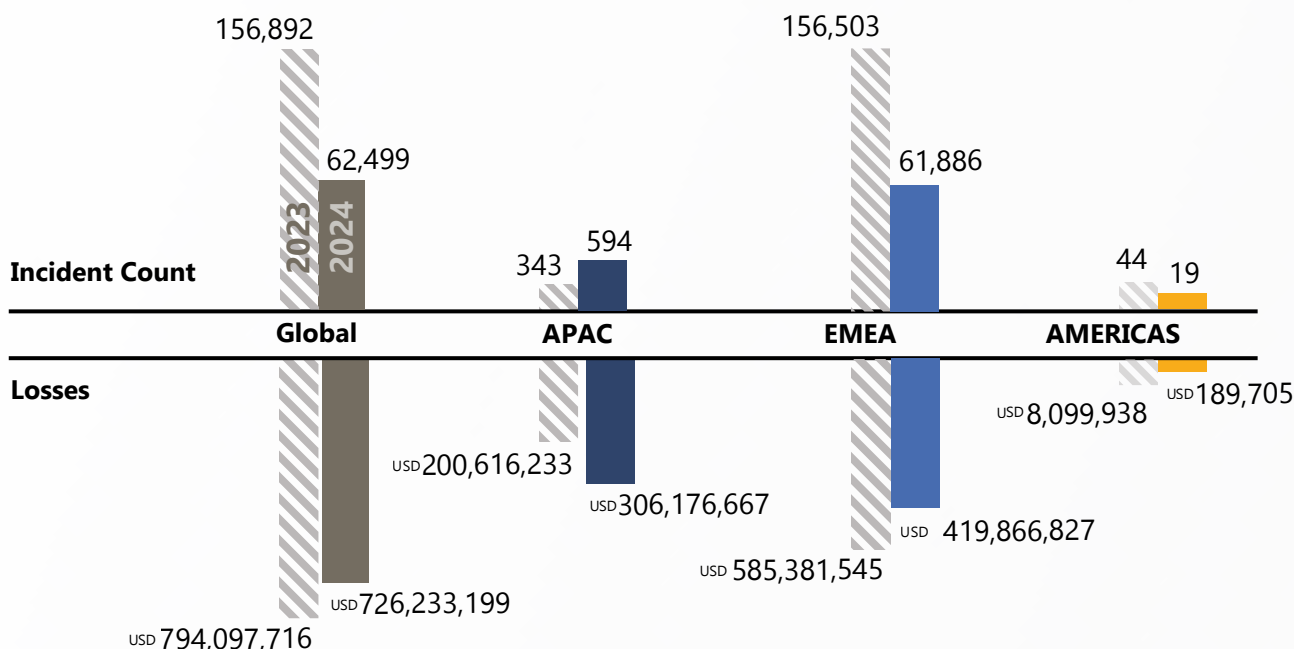
19

Global Cargo Crime Overview

Supply Chain Losses Across the Globe

2024 Reported Global Cargo Incidents & Losses

In comparison with 2023



A Global Look

The total number of incidents at 62,499 shows a decrease by 60% from last 2023, which saw over 156,000 cases. Yet 2024's financial losses continue to be substantial with a small decrease of 8.5%. The difference of incidents reported from 2023 is due to the number of reported incidents from the EMEA region. The trend is largely driven by factors such as high inflation, economic pressures, and geopolitical conflicts including the wars in Ukraine and the Middle East, which together are fueling cargo crimes.

Macroeconomic Pressures and Inflation

High inflation has been cited as a primary driver behind cargo crime patterns, with rapidly rising prices, criminals find higher rewards in targeting high-demand commodities such as high-value electronics in APAC due to most of the manufacturing hubs being stationed in this region.

Geopolitical Instability and Regional Conflicts

Global conflicts and trade disputes disrupt key trade routes, forcing rerouted shipments with longer transit times. This delay of shipments travelling to EMEA create additional opportunities for cargo crime.

Digital Vulnerabilities

The pandemic has accelerated digital transformation in supply chain and logistics while also exposing vulnerabilities for criminals to exploit. An example of this case is a recent data breach of a logistics firm. Rapid digitalization has exposed vulnerabilities, like document forgery that criminals exploit to hijack shipments from ports.

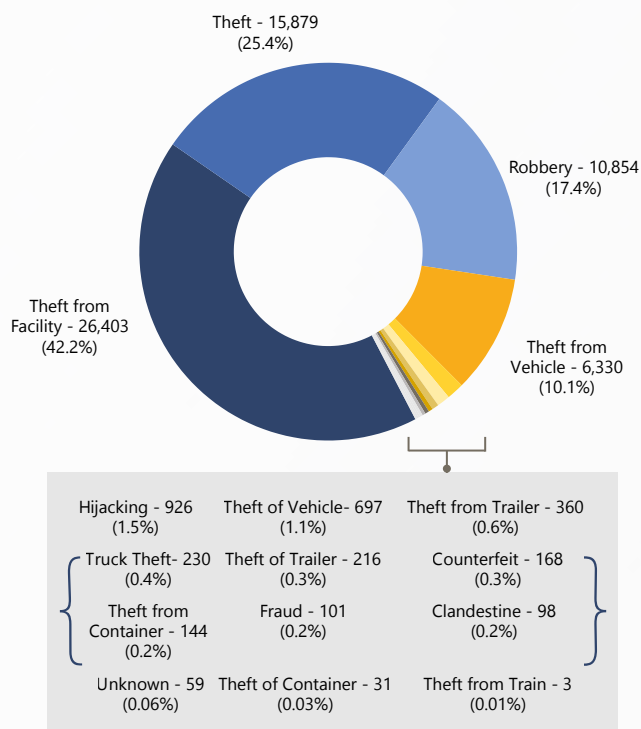
Economic Restructuring and Nearshoring Trends

Shifts in global manufacturing, including a move toward nearshoring, have led to increased cargo volumes in transit. Meanwhile, the AMERICAS region has experienced losses due to higher value cargo shipments being increasingly targeted.

Global Cargo Crime Trends

Cargo Crime Insights by Type

By Incident Category

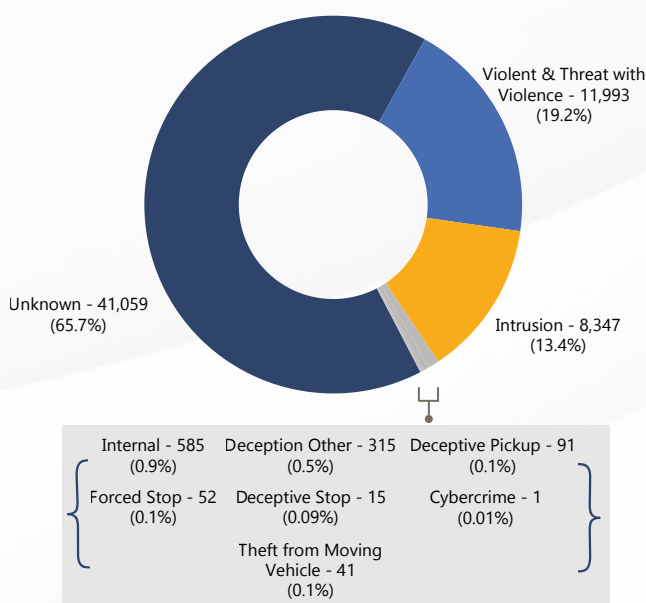


Theft from facilities is the most prevalent category type, accounting for over 40% of all recorded cargo crimes.

Criminal organizations are increasingly targeting points of origin and warehouse storage facilities, taking advantage of limited staffing and weak security during late-night hours. Internal related thefts further increase the risk of perpetrators bypassing security measures, these are most frequently done through the involvement of internal staff, truck drivers, and third-party security guards.

INTERNAL EMPLOYEE INVOLVEMENT CASE >

By Modus Operandi



TIS has observed an increase in 'Unknown' modus operandi, indicating that criminal groups are finding new ways to evade detection. This trend shows how criminals continuously change their tactics to elude existing security measures.

The second most reported method involves "Violence/Threat with Violence," with over 19% of reported incidents, often the preferred method used for incident categories such as theft, robbery, facility theft, vehicle theft, and hijacking. Criminal groups target areas with a lack of surveillance and understaffed security teams, making these locations easy targets for violent thefts.

TIS recommends companies to utilize AI based security systems that can help in the detection of unknown individuals or visitors entering the vicinity of the facility.

Largest Single Incident in Asia Pacific

Six Arrested in USD 4.2M Laptop Heist at Chennai Port

 Chennai, India  September 2024  USD \$4,200,000

Six persons have been arrested in connection with a heist at Chennai Port Trust, where a group of individuals managed to steal laptops worth ₹35 crore (USD 4.2M), police stated. Authorities recovered 5,207 stolen devices along with the container and the trailer lorry used in the crime.

The group allegedly forged transport documents to unlawfully collect the container from a yard inside Chennai Port Trust soon after it was imported via a foreign vessel earlier that month.

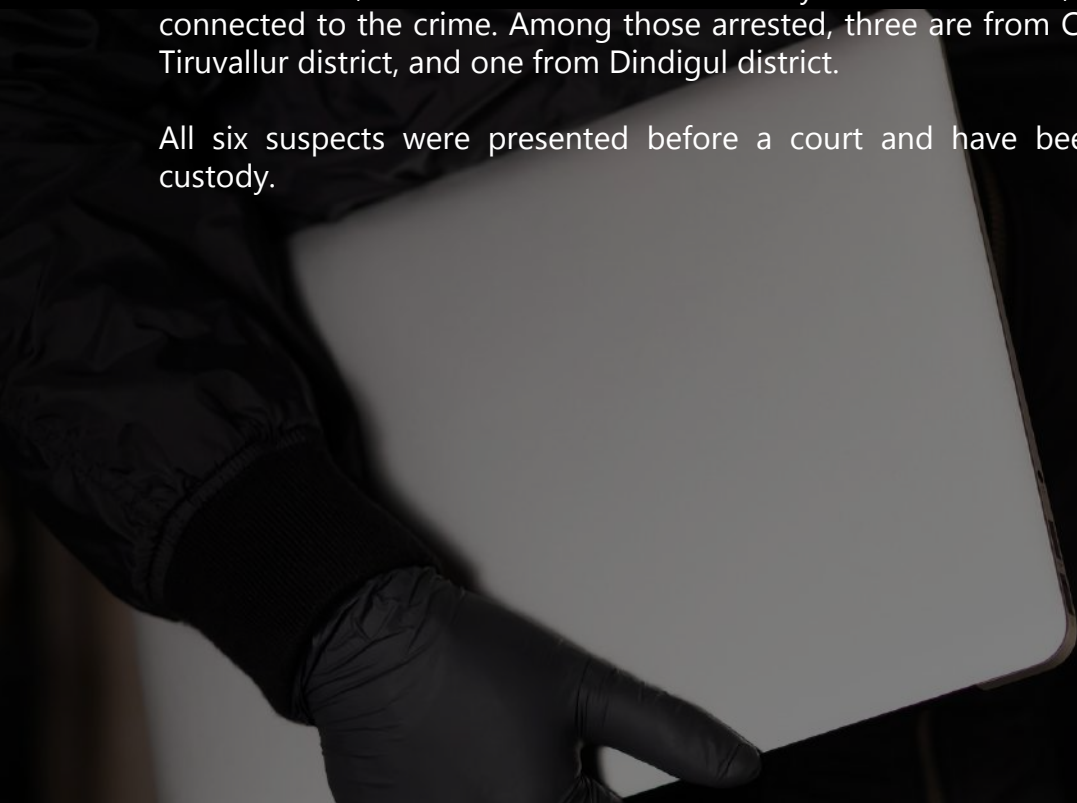
The theft was discovered on September 11 when the operations manager of a private firm, arrived to collect the container. The records indicated that the container had been handed over to the consignee, but the manager found it missing. The container, which arrived at the port on September 7, had been offloaded at the yard before it was stolen.

The manager reported the incident to the Harbour police, who quickly determined it was an inside job. Investigators found that the transport documents used to claim the container had been forged using insider knowledge of the shipment details.

The probe led police to an employee of the handling firm. "The investigation revealed that the employee had forged the necessary documents to collect the container and passed them to his accomplice. The accomplice then submitted the fabricated documents to the port and successfully removed the container using a trailer lorry," police said in a statement.

Authorities located the stolen container and the lorry used in the crime. The six suspects were arrested, while a manhunt is underway for three others, including the employee connected to the crime. Among those arrested, three are from Chennai district, two from Tiruvallur district, and one from Dindigul district.

All six suspects were presented before a court and have been remanded to judicial custody.



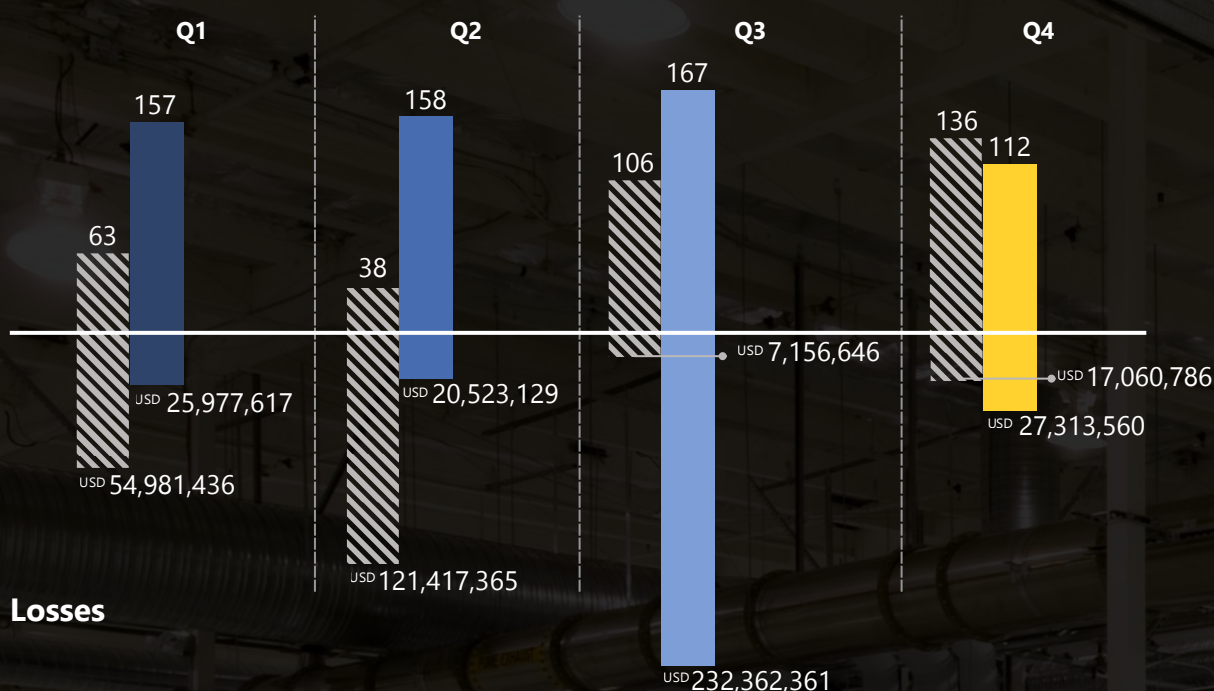
Asia Pacific Per Quarter Analysis

Comparing 2024 and 2023 Data by Quarter

2024 Incidents & Losses by Quarter

In comparison with 2023

Incident Count



Losses

2023 Biggest Case: Organized Truck Theft of Imported Coal worth USD 120 Million

[READ 2023's BIGGEST LOSS INCIDENT >](#)

2024 Biggest Case: Six Arrested in USD 4.2M Laptop Heist at Chennai Port

[READ 2024's BIGGEST LOSS INCIDENT >](#)

Cargo Crime Incidents Peaked in Q3 of 2024

TIS data identifies Q3 as the most critical period for cargo crime in 2024, with the highest incident count and financial losses.

In comparison, 2023 recorded the highest incident count in Q4, while the greatest financial losses occurred in Q2 due to a large-scale incident.

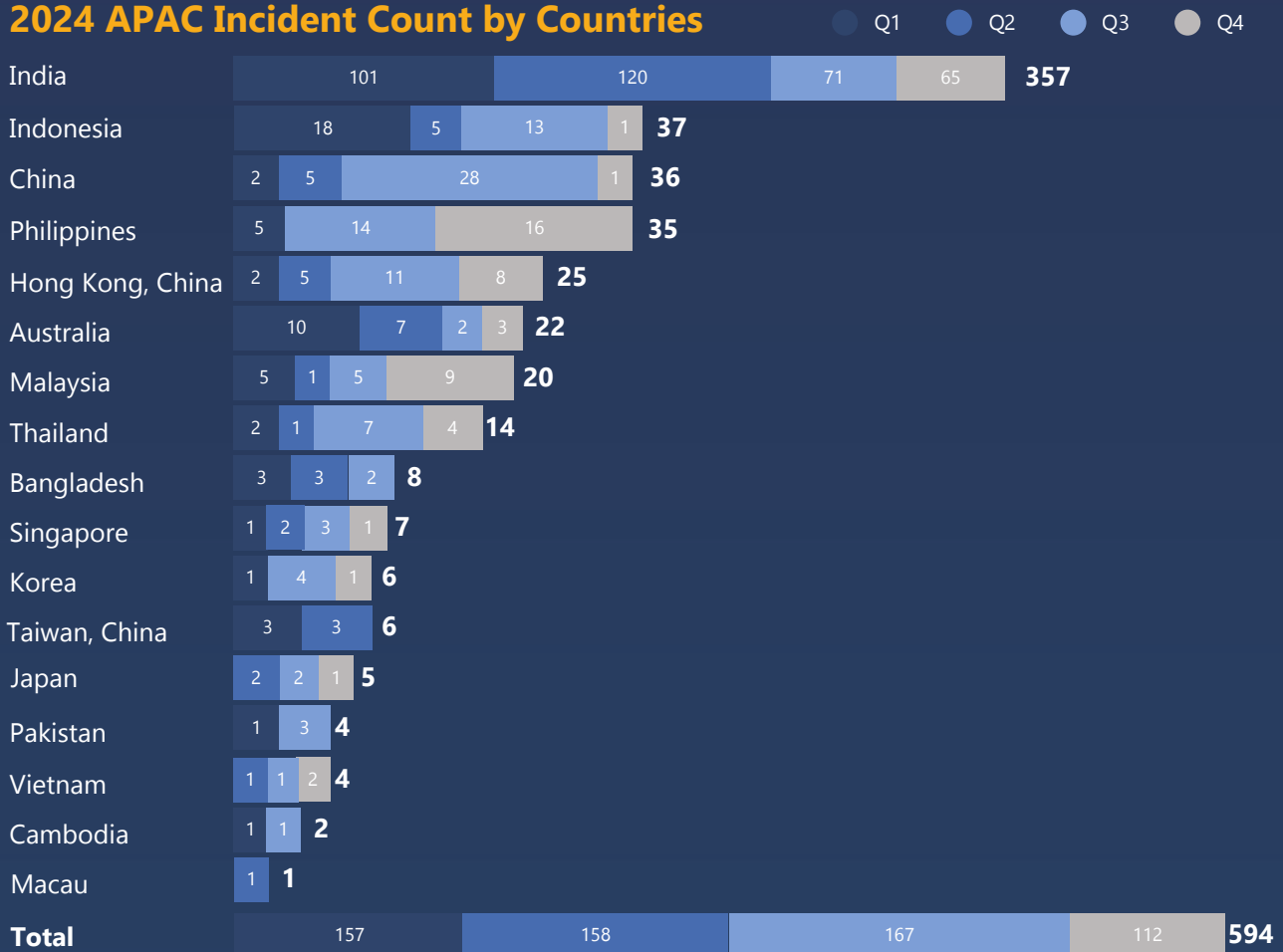
As Q3 ushers in the holiday season, businesses ramp up production and distribution to meet rising consumer demand, leading to a surge in high-value shipments. This increased shipping activity strains logistical systems, creating security gaps that criminals exploit. With expedited shipments and frequent deliveries, more goods are in transit or stored at logistics hubs, making them prime targets.

The operational pressures of peak season can also result in lapses in security measures, especially in understaffed facilities with reduced monitoring, a vulnerability that organized crime groups strategically exploit. As companies rush to fulfill market demand, security protocols may be overlooked, increasing the risk of cargo theft and interception by criminal groups.

Asia Pacific Cargo Crime Trends

Cargo Crime by Country Analysis

2024 APAC Incident Count by Countries



Disclaimer: All incident cases included in this report have been verified and sourced from publicly available information and incidents reported by members. Accuracy on number of actual cases is not guaranteed.

India leads with the highest reported incidents, accounting for 60% of the region's total recorded incidents in 2024. As India emerges as a formidable manufacturing hub in APAC, its vast geographic expanse complicates efforts to regulate operational threats effectively. This situation shows the need for enhanced protocols, especially in rural areas where shipments are en route and storage warehouses operate. Implementing robust standards such as the TAPA Facility Security Requirements (FSR) can address vulnerabilities in asset storage, while the TAPA Trucking Security Requirements (TSR) supports cargo threat mitigation during shipment delivery, together providing a stronghold to keep operational functions safe.

Cargo crime incidents in Indonesia, China, and the Philippines stem from various factors. Indonesia's vast archipelago complicates risk mitigation, creating opportunities for theft. China's high cargo volume and industrialization contribute to incidents despite strict enforcement. The Philippines struggles with fragmented logistics due to its island geography and developing infrastructure. Other countries like Hong Kong, Australia, and Malaysia show notable figures, while lower numbers were seen in Thailand, Bangladesh, and Singapore, with single-digit reports in Korea, Taiwan, and Japan. These variations require strong risk strategies to safeguard supply chains.

By Incident Category: Facility Related Cargo Crime & Rampant Fake Goods

TIS recorded that Theft from Facility is the most reported incident category for the APAC region. This data explains to us the vulnerability of warehouses and storage sites which remain the prime targets for criminal groups.

This data agrees with what TIS recorded for 2023 for the APAC region, which showed that Theft from Facility remains as the topmost targeted category.

Warehouses often store high-value goods in large volumes, making them prime targets when security measures are insufficient. Moreover, internal-related

theft amplifies these risks. Criminal organizations capitalize on insider access, recruiting or coercing employees, truck drivers, and even third-party security guards to bypass safeguards undetected. Insiders have direct knowledge of facility layouts, shipment schedules, and security routines, allowing them to plan thefts with minimal resistance. Such schemes can involve forging documentation, manipulating inventory records, or simply taking advantage of blind spots in surveillance.

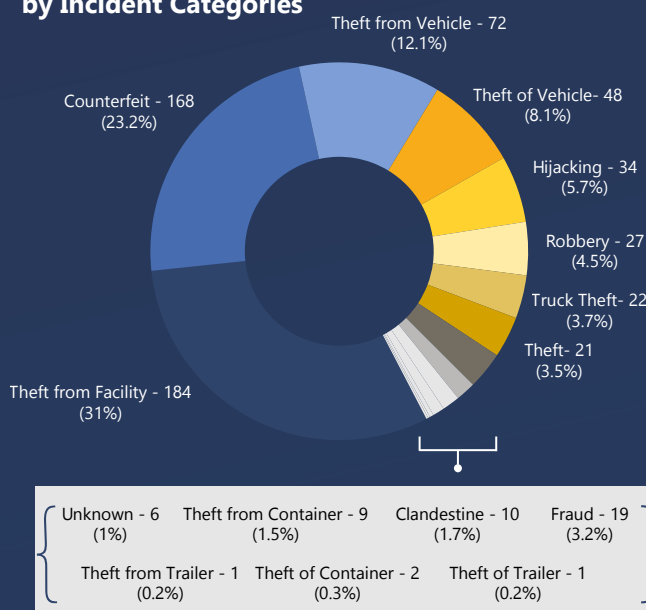
Counterfeit goods have emerged as the second-highest incident category in 2024, with over 23% reported cases. The rapid expansion of eCommerce platforms has created a larger market where counterfeit products can proliferate. As online marketplaces grow, they often struggle to enforce strict quality controls and verification processes across a vast number of sellers, making it easier for counterfeiters to operate. In addition, the economic pressures and supply chain disruptions experienced over recent years have incentivized some criminal groups to adopt counterfeiting as a lower-risk, high-reward venture.

Transportation Related Cargo Crime & Use of Fraud

"Theft from Vehicle" ranks prominently with 72 reported incidents, which closely ties with Theft of Vehicle and Hijacking, effectively totaling over 154 of incidents related to transportation of goods. According to TIS reports, criminal strategies for vehicle-related theft often involve internal connections, driver bribery, and meticulous monitoring of delivery schedules to facilitate the hijacking and theft of high-value goods.

Lesser-reported categories, such as fraud, clandestine activities, and container-related thefts, offer insights into the tactics used by criminal groups. For instance, a notable 2024 case involved fraud through forged documents to claim a shipment. Another case revealed clandestine practices where genuine goods were swapped with substandard or altered ones, allowing criminals to steal assets without immediate detection.

Breakdown of 2024 APAC Incidents by Incident Categories



Internal Employee Involvement Case

Sydney Employee Charged for Theft of 8,000 Solar Panels Worth USD 780,000

 Australia

 August 2023

 USD \$780,000

New South Wales Police have charged a 37-year-old man in connection with the theft of nearly 8,000 solar panels, valued at AUD\$1.2 million (USD 780,000), from his employer in western Sydney.

The investigation began in August after a local business in Minchinbury reported the discovery during an internal audit that revealed the panels were missing from its warehouse.

Authorities allege that between May 9, 2023, and August 9, 2024, the employee sold 7,894 solar panels to third parties without the company's authorization or knowledge.

Following the inquiry, detectives from the Mt Druitt Police Area Command arrested the suspect. He has been charged with stealing and unlawfully disposing of property.

The accused has been granted conditional bail and is scheduled to appear before Mount Druitt Local Court.

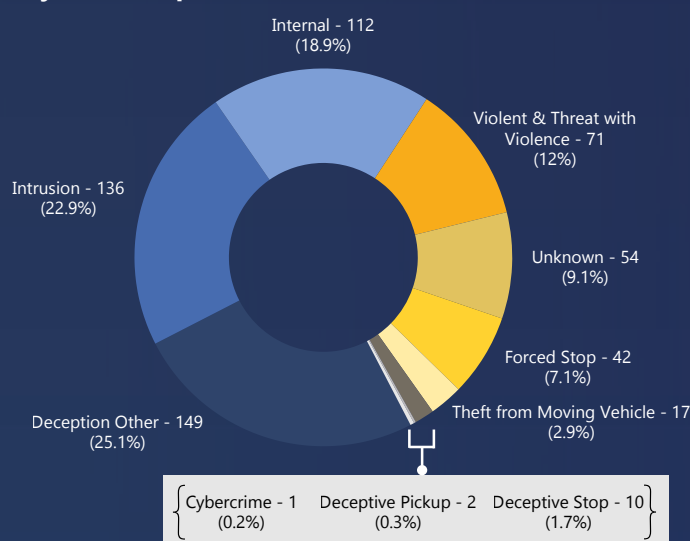
Modus Operandi Trends: Deception, Intrusion, and Internal Employee Involvement

Deception Other accounted for over 25% of incidents, refers to the various methods of masking, falsification, and trickery aimed at making shipments appear legitimate while remaining undetected. The data shows a rise in counterfeit products and fake cargo infiltrating the supply chain.

Intrusion, at 22%, follows closely behind, with TIS identifying it as the top modus operandi for all recorded incidents in 2023. The number of recorded intrusion-based incidents rose by 41% in 2024, largely driven by facility and truck-related intrusion reports. This surge aligns with the

continuous expansion of APAC as a global manufacturing hub, where newly opened facilities often become prime targets for criminal groups. The 3rd most prominent category is "Internal" also known as internal employee involvement accounted for 112 incidents in 2024, a 47% increase compared to 2023's recorded incidents. 2024's recorded incidents showed an increase in insider crimes, often involving warehouse employees, coerced security guards, and drivers collaborating to enable shipments being stolen en-route and bypassing security protocols placed at facilities.

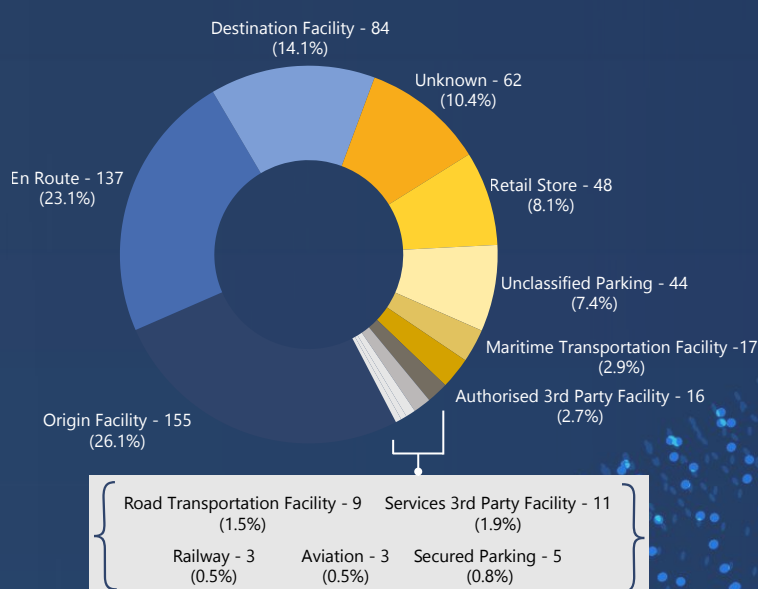
Breakdown of 2024 APAC Incidents by Modus Operandi



[READ THE TIS ANNUAL REPORT 2023 HERE >](#)

Location-based Incidents: Facility and Transportation Data

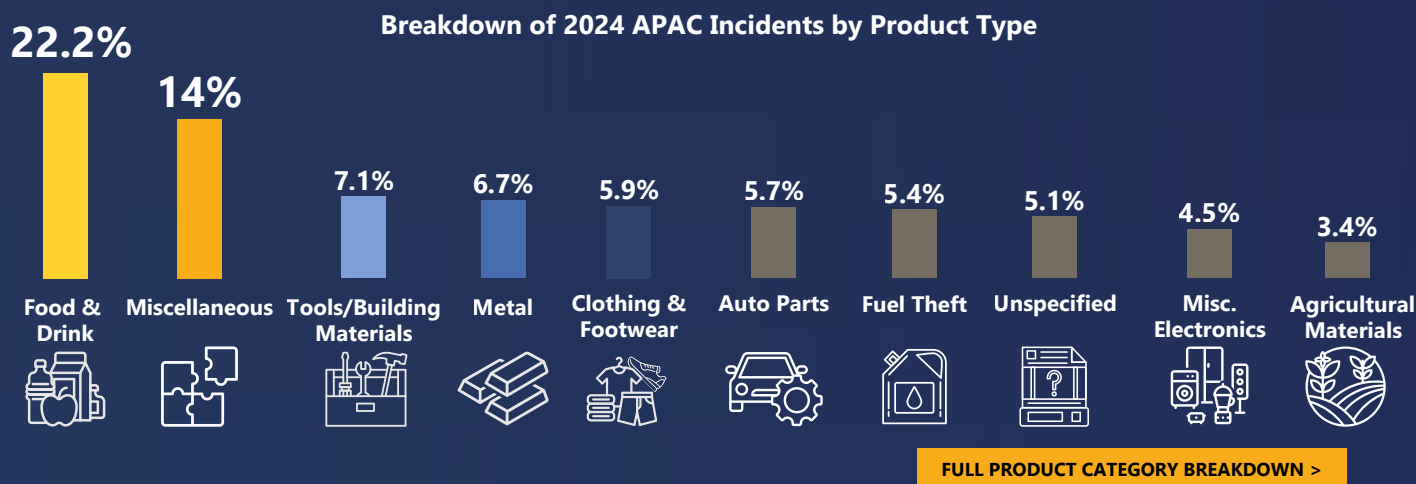
Breakdown of 2024 APAC Incidents by Location Type



Over 26% of cargo crime incidents in 2024 took place at origin facilities, where criminals target goods at their point of creation. Meanwhile, 14% of reported incidents occurred at destination facilities, such as warehouses and storage sites. Criminals anticipate incoming shipments and plan how to access these goods while they are stored before final delivery to customers and other establishments.

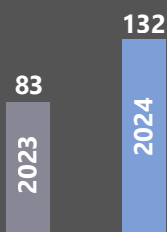
En route incidents accounted for 23% of cargo crime in 2024, while unclassified parking recorded 7%. This data suggests that a significant portion of incidents occur during transit, spanning highways, rest stops, and parking areas.

Top 10 Product Categories Being Targeted



Food & Drink accounted for 22.2% of all reported cargo crime incidents in 2024, an increase of over 59%, with 132 incidents recorded compared to 83 cases in 2023. This increase is due to the high demand for these essential goods, which criminals can quickly resell or redistribute, making them particularly attractive targets. Food prices have risen due to declining domestic production and higher import costs. Climate change has intensified the frequency of extreme weather events, placing additional strain on food systems. In the Asia Pacific region, reliance on food imports, vulnerability to climate disruptions, and rapid urbanization have all contributed to higher demand for consumable goods and increased the risks associated with their transportation.

Incident
Comparison
for
Food & Drink in
2023 versus 2024



Additionally, the modus operandi internal employee involvement accounts to a quarter of all Food & Drink-related incidents, further reminding us of the importance of stricter employee screening to ensure the mitigation of this trend. Recorded incidents indicate that thefts involve not only en-route deliveries but also intrusion-based attempts on warehouse storage facilities.

Following this, Miscellaneous goods at 14% shows the broad range of goods that was lost due to cargo crime. Cargo shipments carrying multiple different type of products and items fall under this category. Tools/Building Materials (7.1%) and Metal (6.7%) reflect a growing focus on industrial goods, likely fueled by global construction and manufacturing demands as countries continue to innovate and advance structural developments. The increasing value of these materials makes them prime targets for theft. A notable incident highlighting the theft of metal and building materials is featured in the TAPA APAC Lookout Magazine December 2024 issue, dissecting the persistent risks faced by this sector.

[MORE ABOUT THIS INCIDENT HERE >](#)

A TIS Case Study

Improving Cargo Security Practices in High-Risk Shipments

USD 1.3 Million Worth of Mobile Phones Stolen En Route Without Detection

TAPA APAC Intelligence System (TIS) has observed a recent major incident which occurred on August 15, 2024, involving a high-value cargo hijacking, where GPS tracking systems are compromised, leaving the valuable shipment vulnerable.

A truck transporting 1,500 high-value mobile phones was robbed in India's Sagar District. The heist, valued at USD 1.3 million, occurred over 125 kilometers while the truck was still moving. Despite advanced security measures, including GPS tracking and a high-security container, thieves managed to break in undetected.

According to claims made by the transporters, the driver was drugged and gagged before the heist took place. The hijacking, which occurred while the truck was en route, reflects the methods criminals are now using to target moving shipments. The ease with which locks and alarms were bypassed suggests an urgent need for reviewing and improving the integrity of security devices, especially when dealing with valuable cargo.

Technology Error, Human Factor or Insider theft?

The human factor played a significant role. The alleged drugging of the driver illustrates the ongoing risks associated with personnel, emphasizing the importance of robust vetting, training, and monitoring of drivers. Implementing a buddy driver system, where two drivers are assigned to high-value shipments, could be a useful strategy to enhance security.

"Another probable cause is that the lorry's GPS application username and password were leaked before the delivery started, likely due to improper storage of credentials" shared by Mr. Mazlin Othman, Manager of Corporate Security Division at Kintentsu World Express – a member company of TAPA APAC. The use of shared desktops by rotating shift workers shows this type of risk, as credentials can be carelessly written on small pieces of paper and displayed openly. This type of careless practice exposed critical shipment details, including driver information, to potential misuse.

Ms. Janet Wong Sing Qing, Regional Manager of Project Argus – also a TAPA APAC member company, highlighted several red flags that indicate weaknesses in both technology and human oversight. Despite the truck being equipped with GPS and advanced security systems, no alerts were triggered during the theft. "This could suggest that the GPS system was either tampered with or improperly configured, reminding the need for continuous monitoring and proactive alert systems" Janet stated.

Mazlin further added that scenarios like vital information about the shipment made accessible on a public whiteboard, further increases the likelihood of leaks. With a smartphone, one could capture and share this sensitive information within moments. Despite the presence of security features like a vehicle panic button, no information has been shared about its use, and it remains unclear whether the shipment was being actively monitored during the incident. Furthermore, there is no data available to confirm if a second driver was present.

Risk Management & Resilience: Adherence to TAPA Standards

This case shows the importance of adhering to TAPA's global standards such as Trucking Security Requirements (TSR) and Risk Assessment Standard (RAS). TAPA's TSR Level 1 emphasizes the necessity for robust tracking and locking mechanisms, tamper-proof systems, and integrated real-time monitoring. The failure to trigger alerts in this case demonstrates the need for a multi-layered security approach, including anti-tampering measures and emergency communication protocols.

To mitigate risks and safeguard high-value shipments, a more comprehensive approach to vehicle monitoring and security is needed. Live monitoring should be conducted throughout the shipment's journey in case of abnormalities. Ensuring all personnel involved are adequately trained in monitoring can also make a significant difference shared by Mazlin.

A thorough risk assessment strategy should always precede the deployment of security measures. Risk assessments help identify potential danger zones, such as the 125-kilometer stretch where this incident occurred.

By analysing crime rates and historical data on cargo theft along specific routes, companies can implement preemptive measures such as route adjustments, increased monitoring, and geo-fencing.

For shipments of high-value cargo—like the USD 1.3 million worth of mobile phones in this case—a robust security response is critical. Tamper-proof GPS systems with real-time alerts, especially when the truck deviates from its route or shows signs of unauthorised access, would be indispensable in preventing such thefts.

Strictly following TAPA TSR Standard with these suggested recommendations offers the most robust approach to safeguarding high-value cargo end-route.

Suggested Recommendations Adhering to TAPA Standards

- **Personnel Management:** No unauthorized parties allowed in truck or trailer. The business must have policies and procedures in place to prevent unauthorized parties from being present in truck or trailer.
- **Frequent Password Changes:** A policy should be implemented for all user accounts to manage and control access to Information Systems by using unique individual identifiers and strong passwords. Passwords must be changed every 90 days.
- **Multiple GPS Systems:** A tracking device must be installed in a covert location in the truck/van tractor and, where available, must be capable of utilizing at least two methods of signaling.
- **Controlled Access to Information:** Shipping details should be compartmentalised based on the "need-to-know" principle, limiting exposure to sensitive data. Implementing authorised personnel lists, electronic door access, and CCTV systems with audio capabilities will further control access.

- Security Escort Services: A trained and recognized internal resource or external security company must be utilized for escort of road transport vehicles.
- Refresher Training: Continuous training and awareness programs for drivers, a program in place for staff to include training, appropriate use of tracking devices and other security equipment, and alarm protocols

Utilizing Incident Insights via TIS for Risk Mitigation

TIS's platform provides critical support in incidents like the recent high-value cargo hijacking in India. TIS's system, which specializes in cargo crime data compilation and logistics route assistance, allows companies to track trends, assess high-risk areas, and implement targeted security measures proactively. In this case, where GPS tracking was compromised, TIS's insights into similar incidents help identify vulnerabilities and improve route planning to avoid known hotspots. The platform's analytics can also aid with law enforcement, offering data-backed insights to support in deterring future hijackings. Through historical data, TIS empowers companies to adapt, reinforcing the security of goods in transit and supporting efforts to ensure accountability throughout the supply chain.

Implementing Multi-layered Responses

This incident is a reminder that protecting high-value shipments requires more than just advanced technology. Multi-layered security approaches, including adherence to TAPA's globally recognized standards, human factor considerations, regular risk assessments, and data analytics with TIS, are essential to safeguard against evolving threats. Effective implementation of these strategies ensures that businesses are not merely reacting to threats but proactively mitigating them.

Thank You to the TIS Working Group Members for Their Collaboration on This Article



Mr. Mazlin Othman
Manager of Corporate Security
Division, Kintentsu World Express
TIS Working Group Member



Ms. Janet Wong Sing Qing
Ops Director, Project Argus
TIS Working Group Member

The TIS Working Group is a collaborative initiative designed to advance supply chain data reporting and resilience across the region.

Join the 2025 TIS Working Group

Bringing Together Industry Professionals to Combat Cargo Crime

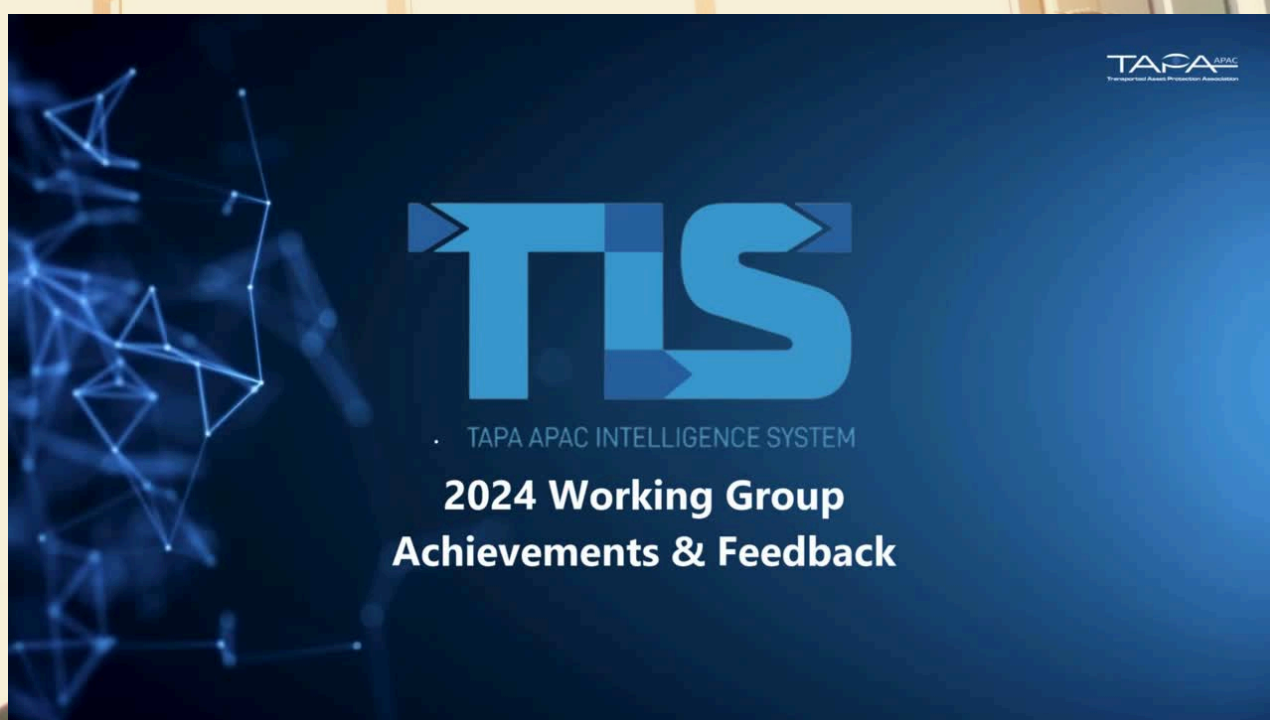
The TIS Working Group plays a vital role in addressing underreported crimes and enhancing industry-wide reporting standards. Established by TAPA APAC, the group is dedicated to improving crime reporting mechanisms, fostering strategic partnerships with Law Enforcement Agencies, and driving industry-wide awareness.

Through its proactive and collaborative approach, the group remains at the forefront of advancing cargo crime reporting, fostering vigilance, and tackling emerging threats within the supply chain industry. Grounded in knowledge sharing, collaborative problem-solving, and best practice exchange, this initiative strengthens crime prevention efforts and reinforces industry security.

Benefits of the TIS Working Group

- Stay informed about Cargo Crime Trends and Issues
- Gaining access to the TIS platform and its risk mitigation features
- Collaborate and connect with local and regional Law Enforcement Agencies, supply chain experts, and partners
- Staying up to date on TIS and upcoming updates to features like the resilient route planning and cargo crime analysis for enhanced supply chain resilience
- Receive Honorary TAPA APAC TIS Ambassador Title & Recognition
- Receive TIS Working Group Member Certificate

Watch the Feedback from 2024 TIS Working Group Members



[APPLY NOW](#)

Insights from TAPA APAC

Combatting Cargo Crime with TAPA APAC

Safeguarding Supply Chains Against Evolving Cargo Crime Threats

The 2024 data provided us with actionable knowledge into the past year's trends of cargo crime, with criminals leveraging multiple tactics to exploit vulnerabilities across the supply chain. APAC's staggering losses of USD \$306 million, despite having a low incident count, reminds companies of the strategic targeting of high-value goods and shipments, particularly at manufacturing hubs and points of origin. Facility theft remains the most prevalent category globally, with insider threats, late-night vulnerabilities, and weak security systems being key enablers.

The most common modus operandi, "Intrusion," and the rising reliance on "Violence/Threat with Violence" reveal that criminals are escalating their methods to overcome security and increase their chances of success. Methods such as deception, fraud, and counterfeit schemes are also prevalent, showing a need for businesses to respond with sophisticated and proactive risk mitigation measures.

Asia Pacific Top Cargo Crime Trends

Surge in Food & Drink Cargo Theft

- In 2024, Food & Drink accounted for 22.2% of all reported cargo crime incidents, reflecting criminals' focus on high-demand goods that can be quickly resold. Rising food prices, climate disruptions, and increased import reliance further exacerbate vulnerabilities, making these essential products particularly attractive targets.

Increase in Intrusion-Based Incidents

- Intrusion was identified as the top modus operandi in 2023 and rose by 41% in 2024, primarily targeting facilities and trucks. As manufacturing hubs expand across Asia Pacific, newly opened facilities face heightened risks due to new criminal tactics and security gaps.

Elevated Insider Threats

- Criminal organizations exploit insider access by recruiting or coercing employees, truck drivers, and security personnel who have direct knowledge of facility layouts and shipment schedules. This familiarity enables them to bypass safeguards, and data shows a rise in such insider-driven incidents in 2024.

Peak Season Preparedness

- Q3 was the most critical period for cargo crime in 2024, showing a marked increase in reported incidents and losses. Heightened consumer demand during the holiday season drives up production and distribution, placing significant strain on logistics systems. This surge in shipments, coupled with operational pressures in facilities and expedited delivery schedules, creates security gaps that criminal groups exploit.

Deception and Counterfeit Shipments

- Criminals increasingly use forgery, false documentation, and counterfeit products to pass off illegitimate cargo as genuine. This enables fraudulent goods to infiltrate the supply chain undetected.

Strategies to Address These Challenges

Risk Mitigation and Resilience with TAPA Standards

- Businesses must invest in robust surveillance systems, advanced tracking technologies, and access control measures to secure both warehouse facilities and goods in transit. Implementing TAPA Standards, such as the Trucking Security Requirements (TSR) and the Facility Security Requirements (FSR), can provide a comprehensive framework for protecting assets in-transit and storage of these goods.

Collaborative Discussion and Data Sharing

- Utilizing the TAPA APAC Intelligence System (TIS) allows stakeholders to exchange and access incident information on cargo crime and criminals' modus operandi, staying informed about emerging tactics used by criminal groups. With TIS, companies can be provided with valuable insights that support supply chain risk mitigation strategies and help combat these incidents.

Combatting Counterfeits with Brand Protection

- The TAPA Brand Protection Standard (BPS) is crucial for safeguarding the valuable brands and intellectual property (IP) by implementing robust measures against counterfeiting and tampering for maintaining consumer trust and brand reputation.

Conducting Risk Assessments

- Complement risk assessment strategies with TAPA Risk Assessment Standard (RAS). A detailed framework that supports a company's risk mitigation strategies. RAS helps companies to assess their end-to-end supply chain risks and prioritize mitigation efforts.

Fortifying the Supply Chain with TAPA APAC

The insights offered from this report focuses on the importance of data-driven decision-making in the supply chain industry. By analyzing patterns and trends, businesses can allocate resources more effectively and stay ahead of emerging threats.

By adopting TAPA Standards, businesses can reinforce operational resilience and counteract threats at every stage of the supply chain, while platforms like TIS ensure that stakeholders stay informed about emerging risks and receive actionable insights for effective mitigation.

“

TAPA APAC remains committed to supporting businesses by delivering actionable intelligence through TIS, promoting best practices, and providing standards to strengthen supply chain resilience across the APAC region.

Tony Lugg

Tony Lugg

Chairperson, TAPA APAC



2024 Statistical Full Breakdown

In descending order

594 Total Reported Incidents

Incident Category

• Theft from Facility	184 (31.0%)
• Counterfeit	138 (23.2%)
• Theft from Vehicle	72 (12.1%)
• Theft of Vehicle	48 (8.1%)
• Hijacking	34 (5.7%)
• Robbery	27 (4.8%)
• Truck Theft	22 (3.7%)
• Theft	21 (3.5%)
• Fraud	19 (3.2%)
• Clandestine	10 (1.7%)
• Theft from Container	9 (1.5%)
• Unknown	6 (1.0%)
• Theft of Container	2 (0.3%)
• Theft from Trailer	1 (0.2%)
• Theft of Trailer	1 (0.2%)

Product Category

• Food & Drink	132 (22.2%)
• Miscellaneous	83 (14.0%)
• Tools/Building Materials	42 (7.1%)
• Metal	40 (6.7%)
• Clothing & Footwear	35 (5.9%)
• Auto parts	34 (5.7%)
• Fuel Theft	32 (5.4%)
• Unspecified	30 (5.1%)
• Miscellaneous Electronics	27 (4.5%)
• Agricultural Materials	20 (3.4%)
• Cash	19 (3.2%)
• Tobacco	19 (3.2%)
• No Load	16 (2.7%)
• Pharmaceuticals	16 (2.7%)
• Phones	14 (2.4%)
• Jewellery/Precious Metals	13 (2.2%)
• Cosmetics & Hygiene	10 (1.7%)
• Furniture/Household Appliances	4 (0.7%)
• Toys/Games	3 (0.5%)
• Computers/Laptops	3 (0.5%)
• Bicycles/Two Wheelers	2 (0.3%)

Modus Operandi

• Deception Other	149 (25.1%)
• Intrusion	136 (22.9%)
• Internal	112 (18.9%)
• Violent/Threat of Violence	71 (12.0%)
• Unknown	54 (9.1%)
• Forced Stop	42 (7.1%)
• Theft from Moving Vehicle	17 (2.9%)
• Deceptive Stop	10 (1.7%)
• Cybercrime	1 (0.2%)
• Deceptive Pick Up	1 (0.2%)

Location Type

• Origin Facility	155 (26.1%)
• En Route	137 (23.1%)
• Destination Facility	84 (14.1%)
• Unknown	62 (10.4%)
• Retail Store	48 (8.1%)
• Unclassified Parking	44 (7.4%)
• Maritime Transportation Facility	17 (2.9%)
• Authorized 3rd Party Facility	16 (2.7%)
• Services 3rd Party Facility	11 (1.9%)
• Road Transportation Facility	9 (1.5%)
• Secured Parking	5 (0.8%)
• Aviation Transportation Facility	3 (0.5%)
• Railway Operation Facility	3 (0.5%)

*Statistics are based on reported incidents to TIS
Actual number of incidents in APAC may be higher



TAPA APAC INTELLIGENCE SYSTEM

**For more information, please email to
tis@tapa-apac.org**



TRANSPORTED ASSET PROTECTION ASSOCIATION ASIA PACIFIC

WWW.TAPA-APAC.ORG/TIS

All Rights Reserved.

Any redistribution or reproduction of part or all the contents in any form is prohibited. You may not, except with our express written permission, distribute or commercially exploit the content.