January 2026

TT Club Loss Prevention

Supply chain security bulletin

What's inside?

Contents

Supply chain security bulletin

This bulletin considers all aspects of supply chain security, highlighting TT Club claims statistics along with a range of other industry data offering an invaluable insight into the current risks facing those tasked with managing security through the supply chain. The Club has produced several reports and guidance documents related to this area of risk across many media platforms.

This bulletin presents a selection of TT Club content and publications as well as highlighting collaborative work undertaken with other like-minded organisations in this space.

The entire library of TT Club's loss prevention guidance can be found at www.ttclub.com/loss-prevention. Please email us at riskmanagement@ttclub.com or get in touch with your usual contact should you have any queries, ideas or suggestions.

Foreword

In an era where global supply chains underpin the movement of goods and the prosperity of nations, the threat posed by freight crime has never been more acute or more complex. The pages of this bulletin outline the evolving tactics of organised crime, the ingenuity of opportunistic thieves, and the persistent vulnerabilities that exist at every stage of the logistics journey – from ports and railways to warehouses and the open road.

No single entity can hope to address these challenges in isolation. The sophistication and global scale of freight crime demand a collective response – one that unites shippers, carriers, insurers, logistics providers, and technology partners in a shared mission. Yet, the responsibility does not end with industry alone. Governments and international bodies must also play a pivotal role, harmonising regulations, sharing intelligence, and investing in the infrastructure and enforcement necessary to deter criminal activity across borders.

Collaboration is the cornerstone of effective supply chain security. It is only through open communication, the sharing of best practices, and the pooling of resources that we can build the resilience required to withstand the threats of today and tomorrow. Whether it is combating the surge in rail theft in the United States, addressing the risks of cargo crime in Morocco and the Middle East, or countering the rise of cyber-attacks and insider threats, our collective vigilance and cooperation are essential.

This bulletin highlights not only the risks we face but also the innovative solutions and collaborative initiatives that are making a difference. From forensic marking technologies and advanced monitoring systems to cross-sector seminars and intelligence-led risk management, the path forward is clear: together, we are stronger.

Josh Finch
Logistics Risk Manager TT Club

Urgent measures needed to combat US rail theft

Rail cargo theft in the USA has become a significant and rapidly evolving threat to supply chains, with recent years seeing an increase in both the frequency and sophistication of such crimes.

Industry statistics show that rail cargo theft incidents have surged, with estimates suggesting a growth of up to 1,500% since 2021. Average losses per incident often reach hundreds of thousands of dollars, and some freight forwarders are reporting up to 100 incidents per day.

The sheer volume of thefts – both by petty thieves and organised criminal gangs – underscores the scale of the problem and the urgent need for effective countermeasures.

Why rail theft is growing

In recent years rail operators have invested heavily in yard security, but this has shifted the problem to other stages of the journey. Thieves now often target moving trains, exploiting sections of track where trains slow down due to terrain or operational constraints.

Tactics include disabling traffic control devices, placing obstacles on tracks or cutting brake lines to bring trains to a halt. Once stationary, criminals board the train, break into containers and transfer the stolen goods into getaway trucks. The use of surveillance, heavily armed gangs and rapid communication networks further enhances the effectiveness of these thefts.

Various factors contribute to the vulnerability of rail cargo in the USA. The vast geography of the country means freight trains often cross remote and sparsely populated areas, particularly in the western and southwestern states. These areas are frequently unmonitored and difficult for law enforcement to patrol, providing ample opportunity for thieves to operate with impunity.

Moreover, the physical characteristics of freight trains present challenges. Trains can be over 5 km long, making them difficult to monitor and protect.

Organised crime

The rise in rail theft is not merely the result of opportunistic criminals but is increasingly driven by organised crime networks. The involvement of international criminal organisations, including those with roots in South America and Eastern Europe, adds a further layer of complexity, with some networks organising thefts to order and coordinating activities across borders.

The technological dimension of rail theft is increasingly prominent. Criminals use drones for surveillance, employ advanced tools to breach containers and exploit vulnerabilities in digital systems to misdirect cargo or compromise shipment integrity. The interconnected nature of supply chains makes it challenging to maintain robust cybersecurity across all partners, increasing the risk of hacks.

Insider threats also play a significant role. Some thefts are helped by individuals with access to cargo manifests and shipment details, enabling targeted attacks on high-value containers. The use of high-security seals, intended to deter theft, can also signal that a container contains valuable goods.

Impact on supply chains

The consequences of rail theft are far-reaching, affecting not only the immediate victims but also the broader supply chain. Transport and logistics companies face significant financial losses, increased insurance premiums and reputational damage.

Businesses have responded by altering their logistics strategies, opting to avoid rail transport altogether or investing in enhanced security measures such as armed escorts, container tracking and environmental monitoring devices. However, these solutions are costly and not universally effective, and the burden of proof in recovering stolen goods remains a persistent challenge.

The legal framework governing rail cargo in the USA adds to the problems. Multi-jurisdictional issues arise as trains cross state lines, complicating law enforcement responses and liability determinations. While current legislation imposes liability on rail operators for theft incidents, some however are attempting to defend such claims by invoking one of the statutory exceptions, arguing these events constitute force majeure.

Addressing the problem

Efforts to address rail theft at the federal level have been limited. While tampering with traffic control devices is now a federal crime, enabling more aggressive law enforcement action, broader legislative reforms are still pending. The Department of Homeland Security has been tasked with addressing freight crime but its response has been largely reactive, focusing on post-incident investigations rather than proactive prevention.

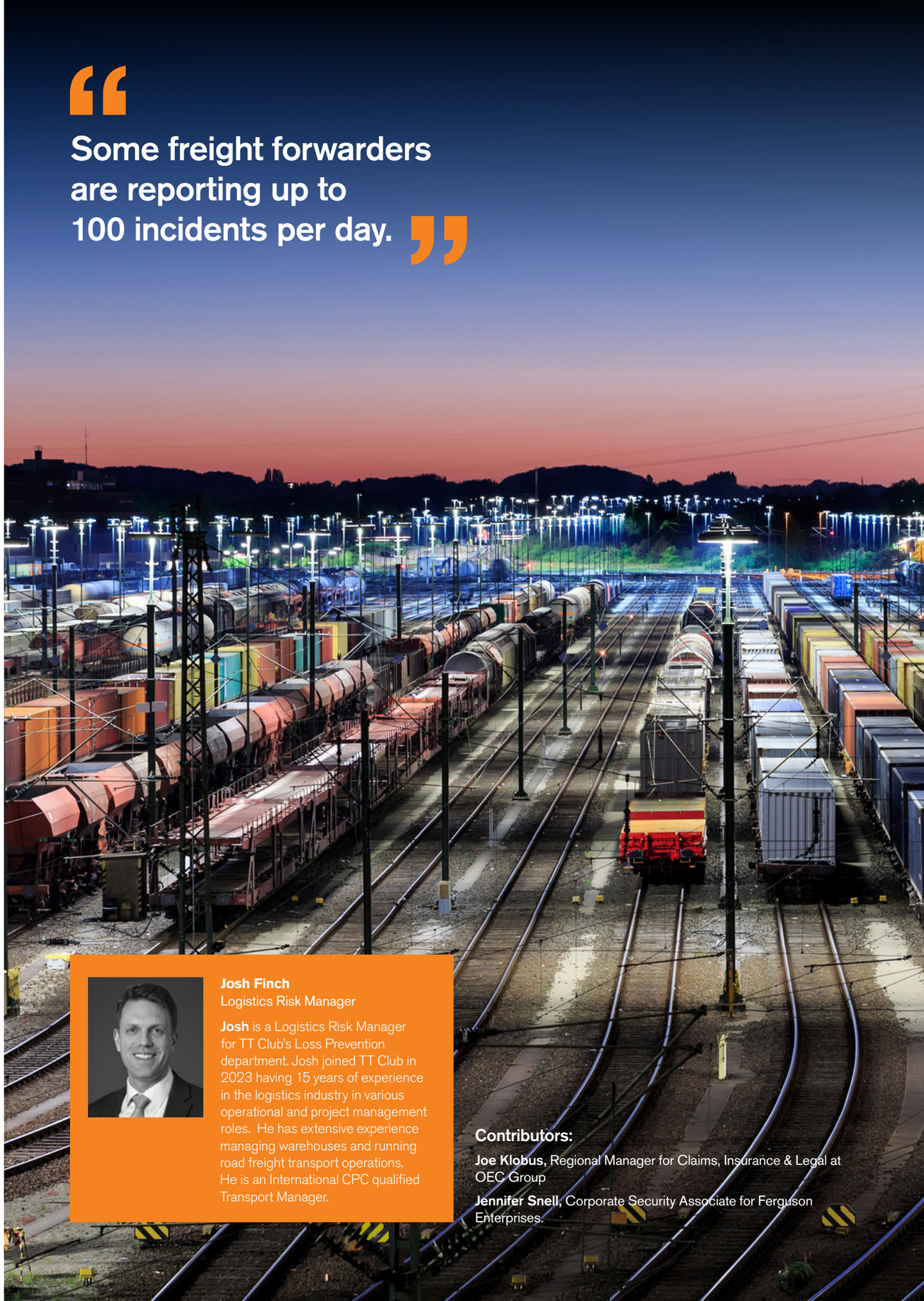
Mitigating the risk of rail theft requires a multifaceted approach. Physical security measures, such as strategic container stowage and the use of robust seals, can deter thefts but may also inadvertently attract attention. Technological solutions, such as container tracking, environmental monitoring and cybersecurity enhancements, offer more layers of protection but are not foolproof. The cost and complexity of implementing these measures, particularly for smaller operators, pose significant barriers.

Industry collaboration and information sharing are essential. The supply chain community must work together to develop best practices, share intelligence and advocate for legislative reforms that address the unique challenges of rail theft. Only through coordinated action can the industry hope to stem the tide of this growing threat.

Conclusion

Rail theft in the USA is a complex and evolving risk, driven by organised crime, technological innovation and systemic vulnerabilities in the supply chain. The scale of the problem demands a concerted response from industry, law enforcement and policymakers alike.

While progress has been made in enhancing security and raising awareness, much more needs to be done to safeguard the nation's rail cargo and ensure the resilience of its supply chains.



> **Some freight forwarders are reporting up to 100 incidents per day.**

Josh Finch
Logistics Risk Manager

Josh is a Logistics Risk Manager for TT Club's Loss Prevention department. Josh joined TT Club in 2023 having 15 years of experience in the logistics industry in various operational and project management roles. He has extensive experience managing warehouses and running road freight transport operations. He is an International CPC qualified Transport Manager.

Contributors:

Joe Klobus, Regional Manager for Claims, Insurance & Legal at OEC Group

Jennifer Snell, Corporate Security Associate for Ferguson Enterprises.

Keep watching out for hostage load scams

The global transport and logistics industry is plagued by many types of theft, but the 'hostage load' scam stands out for its complexity and unique challenges.

Unlike straightforward thefts, where goods and thieves simply vanish, hostage load scams involve the deliberate withholding of cargo by those entrusted to look after it. They then demand payment or resolution of a dispute before releasing the goods.

Awareness, due diligence and clear communication are the keys to building resilience against this persistent supply chain risk.

How hostage load scams work

A hostage load scam occurs when a party in possession of freight – most commonly a carrier – refuses to deliver the cargo to the intended recipient. Instead, they hold the goods as leverage, demanding payment or settlement of a dispute as a condition for release.

The reasons given for such actions can vary widely, from claims of unpaid invoices on earlier shipments to alleged breaches of contract. While there are occasions where genuine civil disputes exist, the practice of withholding cargo has increasingly become a criminal activity.

What makes hostage load scams particularly tricky is the way they blur the line between civil and criminal matters. On the surface, these incidents can appear to be business disputes, but there is often an underlying attempt to extort funds or concessions through unlawful retention of goods. This ambiguity can make it difficult for victims to get help from law enforcement, which may initially view the matter as a contractual disagreement rather than a criminal offence.

Hostage load scams are distinguished by ongoing communication between the scammer and the freight broker, shipper or consignee. This might seem to be an opportunity for intervention, but the scammers are typically good at hiding their identities and operations. They often work through layers of intermediaries, use dispatch phone numbers and enlist drivers who are unaware of the scam.

Occasionally, the scammers do deliver the cargo – usually after a ransom has been paid and when the cargo consists of lower-value goods or those that are difficult to store or sell. Unfortunately this selective fulfilment encourages the idea that paying up can resolve such situations, thereby continuing the cycle.

Why they keep happening

The enduring appeal of the hostage load scam lies in its ability to seem like a civil dispute. The reluctance of law enforcement to get involved emboldens scammers, who know that the odds of prosecution are slim unless there is clear evidence of criminal intent.

The scam is often carried out by carriers with a history of dodgy practices, such as double brokering or operating as 'chameleon carriers'. These entities may appear genuine, but in reality they are controlled by individuals who manipulate multiple companies to obscure their criminal activities and continue operations even after being flagged for misconduct.

There is also growing evidence that organised groups are behind many of the more sophisticated hostage load scams. In some cases, multiple carriers band together, pooling resources and information to maximise their leverage over victims.

What needs to be done

Given the complexity and persistence of hostage load scams, transport and logistics businesses must adopt a proactive approach to risk management. Rigorous due diligence and robust supply chain visibility are essential. Carriers engaging in hostage load scams often show red flags before resorting to such tactics. Thorough vetting of carriers, keeping clear documentation and ensuring that all parties in the supply chain are trustworthy can significantly reduce exposure.

Communication is also crucial. Shippers should work closely with their partners to verify the identity of drivers and equipment, and to document every stage of the delivery process. Any discrepancies or irregularities should be investigated promptly, and suspicious behaviour should be reported to the relevant authorities.

While it may be tempting to pay a ransom in the hope of recovering valuable cargo, this approach only serves to incentivise further criminal activity. Paying a ransom not only encourages scammers but also signals to others that such tactics can be successful.

When engaging with law enforcement, it is important to describe the incident in clear terms. Avoid using terms that may imply a civil dispute and instead say plainly that the cargo has been stolen. This increases the likelihood that the matter will be treated as a criminal offence, rather than being dismissed as a contractual disagreement.

Notwithstanding the above measures, the greatest weapon against the threat of hostage load scams is awareness. Many freight brokers and forwarders may experience such incidents only rarely and not recognise the warning signs until it is too late. By sharing information, documenting incidents and fostering a culture of vigilance, the industry can make it harder for criminals to act with impunity.

Conclusion

Hostage load scams continue to exploit the gaps between civil and criminal law, and between operational complexity and regulatory oversight. By staying vigilant, investing in robust risk management practices and fostering a culture of transparency and cooperation, the transport and logistics industry can significantly reduce the impact of this enduring supply chain threat.

Thanks to James Menges for contributing to this article

James Menges
President of Freight-Intel Network & Defense

How to make supply chains more secure in the Middle East

Over 80 transport and logistics professionals met in Dubai in November to discuss how to improve supply chain security in the Middle East. Hosted by TT Club, the one-day seminar focused on helping Members make regional supply chains more secure through practical risk mitigation, prevention of strategic theft and appropriate due diligence.

The Middle East's growing prominence as a global trade hub has led to a corresponding rise in cargo theft, fraud and security breaches. The seminar provided a mix of technical expertise, legal insight and operational best practice to help attendees – including industry professionals and transport operators – boost the security of their operations.

Elevated threat

Paul Raw, senior security risk and resilience consultant at BSI, used comparative risk mapping to show the elevated threat of cargo theft, hijacking and corruption in the Middle East.

He said the financial impact of criminal activities, particularly the surge in cyber-attacks – which now account for up to 30% of all data breaches, mean there is an urgent need for holistic risk assessment across all tiers of the regional supply chain. According to Raw, only 6% of organisations currently achieve true end-to-end supply chain visibility, with poor visibility staying the top challenge for 2025.

TT Club logistics risk manager Joshua Finch and Dubai office general manager Sudeep Moothedath reinforced the increased need for vigilance, robust training and the adoption of international best practices by discussing some recent claims.

These included the theft of a trailer with high-value furniture, where operational lapses led to significant losses; a copper wire theft helped by a driver who disabled the truck's tracker and fled the country; a hijacking involving fake police, showing the increasing sophistication of criminal tactics; and a fraud case where forged documents enabled unauthorised release of cargo, resulting in ongoing legal proceedings.

> **The financial impact of criminal activities, particularly the surge in cyber-attacks – which now account for up to 30% of all data breaches.**

Legal issues

Omar Omar, partner of international law firm Al Tamimi & Company, provided a legal perspective of cargo crime in the UAE. He explained the criminal liabilities under Federal Law by Decree No. 31 of 2021, including penalties for basic, employee and aggravated theft, as well as fraud and documentation crimes.

Using recent cases, he showed the real-world consequences of insider collusion, forged documents and negligent hiring, with outcomes ranging from prison and fines to loss of insurance cover.

Omar stressed the importance of due diligence in subcontractor vetting, the necessity of written contracts and the corporate duty of oversight. He said failure to watch high-risk staff or to have robust preventive controls could result in gross negligence or complicity charges, and breaking limitation of liability.

Risk mitigation

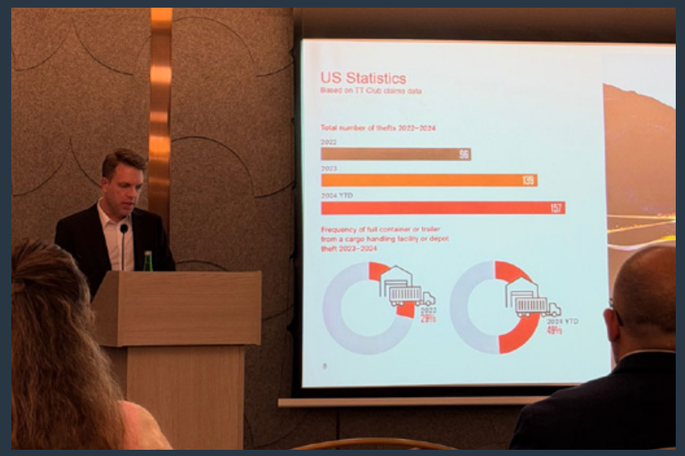
Attendees were encouraged to adopt the core international standards for supply chain security, including ISO 28000 (security management systems), ISO 9001 (quality management) and the NIST Cybersecurity Framework. Together these highlight the importance of robust risk assessment, security governance, prevention and protection mechanisms, and incident response planning.

Supply chain professionals should adopt a proactive, integrated approach – moving beyond superficial compliance to genuine resilience. This should include continuous risk assessment and third-party vendor evaluation, strong access controls and cyber hygiene, regular training and executive sponsorship for security culture, and collaboration with industry groups and regulatory bodies for threat intelligence

In addition, consideration should be given to using artificial intelligence, automation, digital twins and advanced monitoring systems to enhance end-to-end supply chain visibility and security. Decentralised knowledge graphs and advanced risk mapping can also enable organisations to track and respond to risks across thousands of variables and subcontractors.

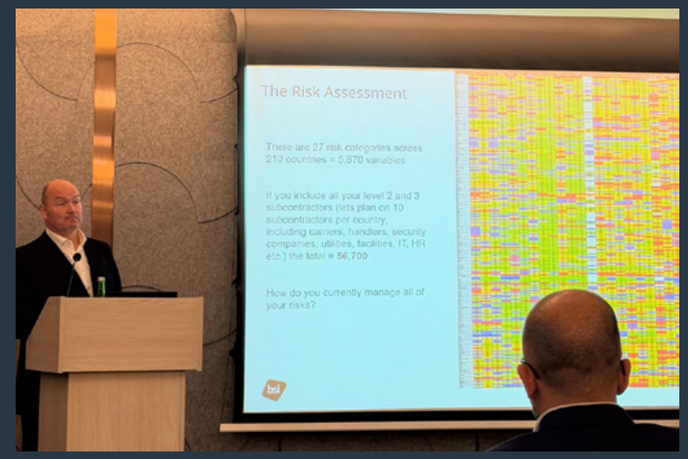
Conclusion

Supply chain security in the Middle East is not merely a compliance issue, it is a business-critical priority. As regional supply chains face unprecedented pressures – from geopolitical instability to technological disruption – the need for collaborative, informed approaches to safety and security has never been greater. TT Club will continue to expand its educational outreach, ensuring Members in the region remain equipped to tackle emerging risks with confidence.



> **Only 6% of organisations currently achieve true end-to-end supply chain visibility.**

> **Supply chain security in the Middle East is not merely a compliance issue, it is a business-critical priority.**



Supply Chain Security & Risk Profile for Morocco

Positioned as a critical logistics crossroads between Africa and Europe, Morocco's strategic importance is anchored by the Port of Tanger Med, the busiest port in the Mediterranean. This geography offers immense commercial opportunity but simultaneously creates a complex, high-risk environment where supply chains are exposed to multifaceted threats.

Information compiled by:
Paul Raw
Senior Consultant, BSI Consulting,
Specializing in Enterprise Risk
& Resilience

Primary Threat

Cargo integrity breaches from illegal drug trafficking, systemic corruption, and stowaway risks pose greater liability than direct asset loss.

Strategic Focus

Sophisticated risk management required to protect against legal, financial, and reputational damage from contraband introduction.

Geographic Intelligence

Specific high-risk zones demand geographically-focused countermeasures and enhanced screening protocols.

Direct Physical Threats to Cargo Assets

In-Transit Cargo Theft & Hijacking

Threat level assessed as Elevated. Criminal tactics are opportunistic, targeting shipments at night or attacking parked containers at unsecured locations. Hijackings typically involve small groups with rudimentary weapons rather than sophisticated syndicates.

Critical Hotspot: Highway A2 connecting Fes and Rabat represents the highest-risk east-west logistics corridor.

Primary Targeted Commodities

- Electronics
- Food products and beverages
- Automotive components
- Clothing and textiles
- Perishables and agricultural products
- Construction materials

Facility Cargo Theft: Assessed as 'Guarded' threat. Incidents are infrequent and geographically limited to the Casablanca-Settat region. Losses are usually partial with low violence levels, though occasional organised attempts using disguises have been reported.

Contraband & Cargo Integrity: The Severe Threat

The co-opting of legitimate supply chains for smuggling operations exposes companies to severe legal, financial, and reputational consequences, including asset seizure, heavy fines, and potential loss of trusted trader status.

1

Illegal Drug Introduction

SEVERE THREAT – Morocco is the world's leading producer of cannabis resin and primary source for European markets. In 2021, authorities seized over **191 tons of cannabis**. Cocaine trafficking threat dramatically increasing, with seizures tripling to over **433 kilograms** in 2021.

2

Stowaway Introduction

ELEVATED THREAT – As primary departure point for migrants attempting to enter Europe, Morocco presents significant security and humanitarian challenges. Stowaways target sea cargo containers and trucks boarding ferries.

3

Counterfeit Goods

ELEVATED THREAT – Morocco is a source country for counterfeit products seized in Europe. Illicit trade costs the government $118 million annually in lost tax revenue. Port of Tanger Med FTZ is critical hub for smuggling and production.

Drug Trafficking Modalities & Geographic Risk

Commercial Road Transport

Concealment in cargo trucks using sophisticated modifications such as false bottoms. Criminals frequently use legitimate commercial goods to conceal narcotics.

High-Risk Products for Concealment:

- Agricultural shipments (fruit, vegetables, meat)
- Food and beverage products
- Furniture
- Automotive products

Sea Cargo

Major consignments seized at seaports, particularly Tanger-Med, followed by Casablanca, Nador, and Jorf Lasfar.

Stowaway Risk Concentration Points

Port of Tanger Med

Primary maritime departure point with highest vulnerability for container and ferry stowaways.

Safi & Casablanca Ferries

Ferries to Spanish ports of Malaga and Algeciras. Port of Safi has particularly inefficient security.

Ceuta & Melilla

Spanish exclaves where attempts are common to access shipments bound for mainland Europe.

Systemic Vulnerabilities: Corruption as Primary Enabler

Operational risks stem from systemic issues where pervasive corruption and regional threats create fertile ground for supply chain disruptions. These vulnerabilities undermine security protocols and compromise officials at critical nodes.

Supply Chain Corruption

HIGH THREAT – Corruption is significant within Morocco's public sector. Historically ineffective anticorruption laws allow state officials to influence organized crime, particularly within the vast cannabis market.

Critical Vulnerability: Port of Tanger Med – corruption among customs and law enforcement is a major concern. Authorities have arrested numerous officials for smuggling involvement. Personnel can be bribed to tamper with surveillance systems.

Terrorism & Organized Crime Nexus

General terrorism threat: **High**.
Supply chain terrorism threat: **Guarded**.

Morocco ranks 27th on African continent for organised crime due to cannabis trade scale, but maintains effective antiorganised crime laws.

Critical Challenge: Drug trafficking networks often facilitated by finances from terrorist organisations, creating a nexus perpetuating both criminal and security threats.

Counterterrorism Strategy: Morocco maintains comprehensive and largely effective approach including vigilant security measures, international cooperation, and robust counter-radicalisation policies. Key initiatives include the King's "proximity strategy" to rehabilitate mosques and train imams, plus hosting UN Office for Counter-Terrorism and Training in Rabat.

Mitigation Framework: Security Measures & Programs

Morocco offers official programs and established best practices that can be leveraged to enhance supply chain security and compliance. A proactive approach can effectively mitigate many identified threats.

1 Moderate Security Baseline

Necessary to counter threats of burglary, robbery, and opportunistic theft across all operations.

2 Stringent Monitoring

Crucial for all cargo departing Morocco, especially shipments destined for Europe, to mitigate severe threat of illegal drug introduction.

3 Chain of Custody

Rigorous and unbroken chain of custody must be maintained and documented for all shipments to prevent unauthorized access and tampering.

4 Address Corruption

Thoroughly vet and address all allegations of corruption within supply chains and among government contacts to mitigate insider threats.

Authorized Economic Operator (AEO) Program

Morocco operates a two-tier AEO program designed to facilitate trade for trusted partners, allowing companies to progressively enhance compliance and security credentials.

Tier 1: AEO Customs Simplification

Active since 2006. No security component. Companies must be financially solvent, transparent, and have no customs infringements.

Tier 2: AEO Security and Safety Status

Added in 2015. Security-focused tier available only to companies with first-tier status meeting additional safety and security standards.

AEO Benefits: Expedited customs procedures, priority processing at ports, and reduced frequency of physical cargo inspections.

Employer Security Practices: Standard security screening practices available in Morocco. Multiple agencies conduct criminal background checks. No known national restrictions prohibit employers from conducting credit history checks or implementing employee drug testing programs.

Strategic Implications: Three Critical Imperatives

Morocco's position as a vital trade hub presents both immense opportunity and significant risk. The security landscape is defined by complex integrity threats that can weaponise entire supply chains, with systemic corruption acting as the primary enabler.

1 Shift Focus from Asset Loss to Integrity Breaches

The gravest risk is not theft, but weaponisation of legitimate cargo for illicit activities. Smuggling of drugs and stowaways, driven by systemic corruption at facilities like Port of Tanger Med, poses far greater financial, legal, and reputational threat than direct asset loss.

Action Required: Prioritise stringent monitoring and chain-of-custody protocols above all else.

2 Geographic Focus is Essential for Effective Mitigation

Risks are not uniformly distributed. Effective route and facility planning must account for specific high-risk zones.

Critical Actions:

- Secure transport along Highway A2 to mitigate hijacking
- Implement enhanced screening and anti-corruption measures at Port of Tanger Med
- Increase vigilance at facilities in Casablanca-Settat region

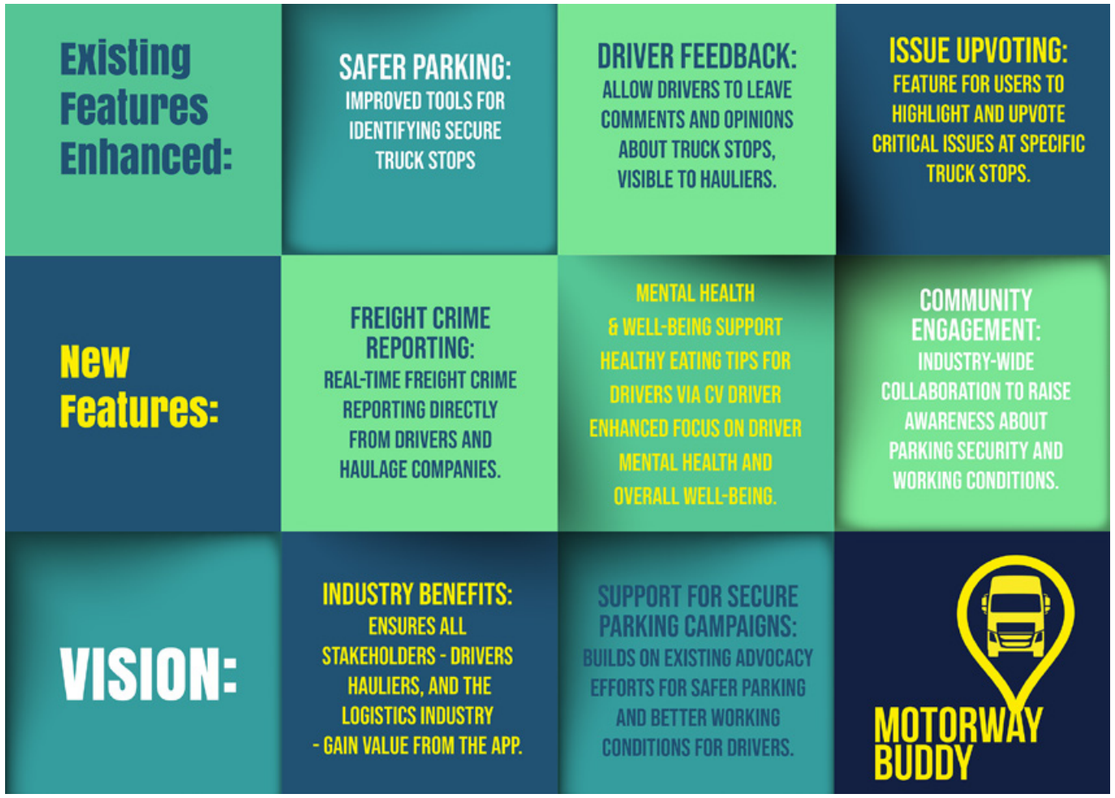
3 Comprehensive Due Diligence is Non-Negotiable

Effective risk mitigation demands a multilayered approach extending beyond physical security.

Success Depends On:

- Active participation in trusted trader programs like AEO
- Implementation of robust anticorruption protocols for all partners and officials
- Vigilant monitoring of CSR compliance to protect physical assets and brand reputation

Conclusion: Success in Morocco's complex supply chain environment requires strategic focus on cargo integrity over asset loss, geographic intelligence for targeted mitigation, and comprehensive due diligence across security, compliance, and CSR dimensions. The intersection of opportunity and risk demands sophisticated, multi-layered risk management to protect both operations and reputation.



Water-based forensic marking offers a cost-effective anti-theft solution

Invisible forensic marking systems can provide a cost-effective anti-theft solution for transport and logistics businesses. Detectable with ultra-violet light, they can robustly tag containers, trailers, vehicles, cargoes and other assets, making them less attractive to criminals. Combined with physical site monitoring systems, forensic marking can provide a valuable extra layer of security to the global supply chain.

Most systems use microdots in an adhesive liquid but one, SmartWater, is water-based and contains coded microscopic particles. Developed in the UK over 25 years ago, it lasts at least five years on outdoor items, is non-toxic and – uniquely – can be manually or automatically sprayed on would-be thieves. The product's effectiveness lies in its ability to link individuals and stolen goods back to the scene of the crime using the liquid's unique code, providing police with hard forensic evidence.

Criminals, aware of the risk of being marked and found, are also less likely to target sites that clearly show they are protected by SmartWater. Independent research in the UK found that 74% of interviewed criminals would avoid committing crimes where SmartWater signage was present, highlighting the psychological impact of the technology.

The solution is already widely used in Britain, where its brand recognition and proven track record – boasting a 100% conviction rate in contested court cases – make it a formidable deterrent. Internationally, SmartWater is deployed in various forms and there are now forensic laboratories in the UK, France and the USA that can read the liquid code.

Supply chain applications

In addition to tagging transport assets and cargoes, water-based forensic marking is particularly useful for deterring thefts of increasingly high-value items such as copper and electrical vehicle (EV) charging cables. The technology is now widely used across solar farms, wind farms and communication sites, as well as in new products like Cable Guard. This is a patented EV cable protection system which incorporates SmartWater in its sheathing – if tampered with, the liquid is released and marks the thief, stolen cable and even the getaway vehicle, providing a comprehensive forensic trail.

DeterTech continues to explore new applications for water-based forensic marking, from ammunition tagging to protecting antiquities in conflict zones. Collaborative development with industry partners is also encouraged, such as integrating SmartWater into security seals or curtain-sided vehicles. This openness to blue-sky thinking invites stakeholders to consider novel ways to enhance supply chain and asset security.

Integrating with physical security

DeterTech also provides physical site security systems to complement its water-based forensic marking solution. In 2019, the company bought PID Systems, a UK provider of perimeter intruder detection systems, followed by Danish temporary site security firm SmartGuard in 2022. Products include the PID 360, a battery-powered 360° mobile monitoring unit with cameras, movement sensors, sirens and lights. Often described as the 'Dalek', these overt surveillance units are widely used in the UK and Europe on construction sites, vehicle parks, goods yards and other secure compounds.

The units detect movement, issue audible and visual warnings, and send video clips to DeterTech's 24/7 alarm receiving centre. This rapid escalation process ensures that any potential criminal activity is quickly spotted and dealt with. Also, with their distinctive blue and yellow chequered design, they are often mistaken for police equipment, further enhancing their deterrent effect. For monitoring larger sites, 5.2 m mobile tower systems with pan, tilt and zoom cameras can work in tandem with PID 360 units.

The combination of mobile camera surveillance and forensic marking creates a layered security approach: any unauthorised presence is detected and recorded while forensic marking ensures that any stolen items or individuals involved can be traced.

Data-led approach

DeterTech also has a crime intelligence department, collecting data from clients, insurance companies and police forces in the UK and Europe. This unique access to police crime data enables the company to build risk matrices, assess vulnerabilities and tailor security solutions to specific sites and threats.

Working closely with organisations such as Opal, the UK's national police intelligence unit focused on serious organised acquisitive crime, the company can request targeted crime data and support live police operations. The resulting strategic focus of 'predict, deter and detect' ensures that the company's security measures are not only reactive but also proactive, predicting criminal behaviour and deploying resources where they are most needed.

DeterTech's DTSentinel is a 5.2-metre-high, rapidly deployable CCTV tower. with AI-powered visual verification and 24/7 monitoring.

Conclusion

Forensic marking systems such as SmartWater can provide an easy and cost-effective way for transport and logistics businesses to protect assets and cargoes from theft. In addition to tagging items – and the criminals who try to steal them – with a unique and traceable code, the warning signage alone acts as strong anti-theft deterrent. Together with mobile site surveillance units and a data-driven approach, water-based forensic marking can provide a valuable extra layer of protection to global supply chains.

> **"Water-based forensic marking can provide a valuable extra layer of protection to global supply chains."**

PID 360 uses motion detection and thermal imaging to identify potential threats, triggering instant alerts.