BSI & TT Club Cargo Theft Annual Report 2018

bsi.

SCREEN
Supply Chain Risk Exposure Evaluation Network

TT CLUB
50 years of established expertise

Table of Contents

Introduction

TT CLUB
50 years of established expertise

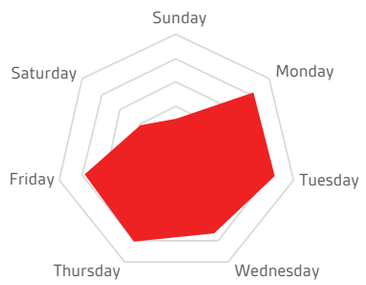
BSI publishes this report in coordination with TT Club.

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

TT Club is the international transport and logistics industry's leading provider of insurance and related risk management services. Established in 1968, the Club's membership comprises container owners and operators (shipping lines and lessors), ports and terminals, and logistics companies, including road, rail and airfreight operators.

As a mutual insurer, TT Club exists to provide its policyholders with benefits, which include specialist underwriting expertise, a worldwide office network providing claims management services, and first-class risk management and loss prevention advice.

Cargo Theft by Day

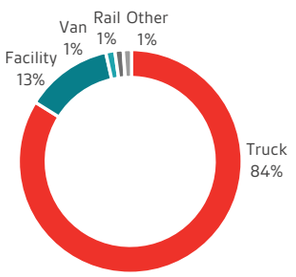


The Club works with some of the world's largest operators down through to companies whose activities are on a smaller scale but face similar risks. Remarkably, in view of industry changes and consolidation, one-third of the membership has chosen to insure with the Club for more than 20 years.

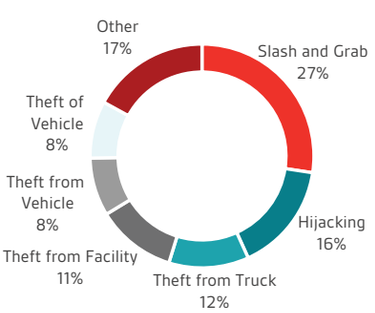
TT Club is managed by Thomas Miller, an independent and international provider of insurance, professional, and investment services.

This report seeks to highlight major areas of concern, targeted modalities and commodities, and theft tactics employed throughout the world. Each organisation has the goal of helping companies stay informed on cargo theft risks in the country, and ultimately, helping prevent freight crimes.

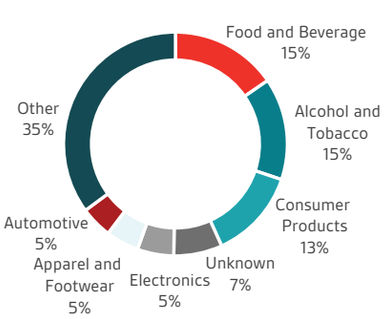
Modalities in Theft



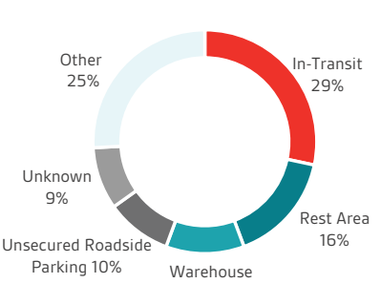
Cargo Theft Types



Top Commodities Stolen



Location of Cargo Theft

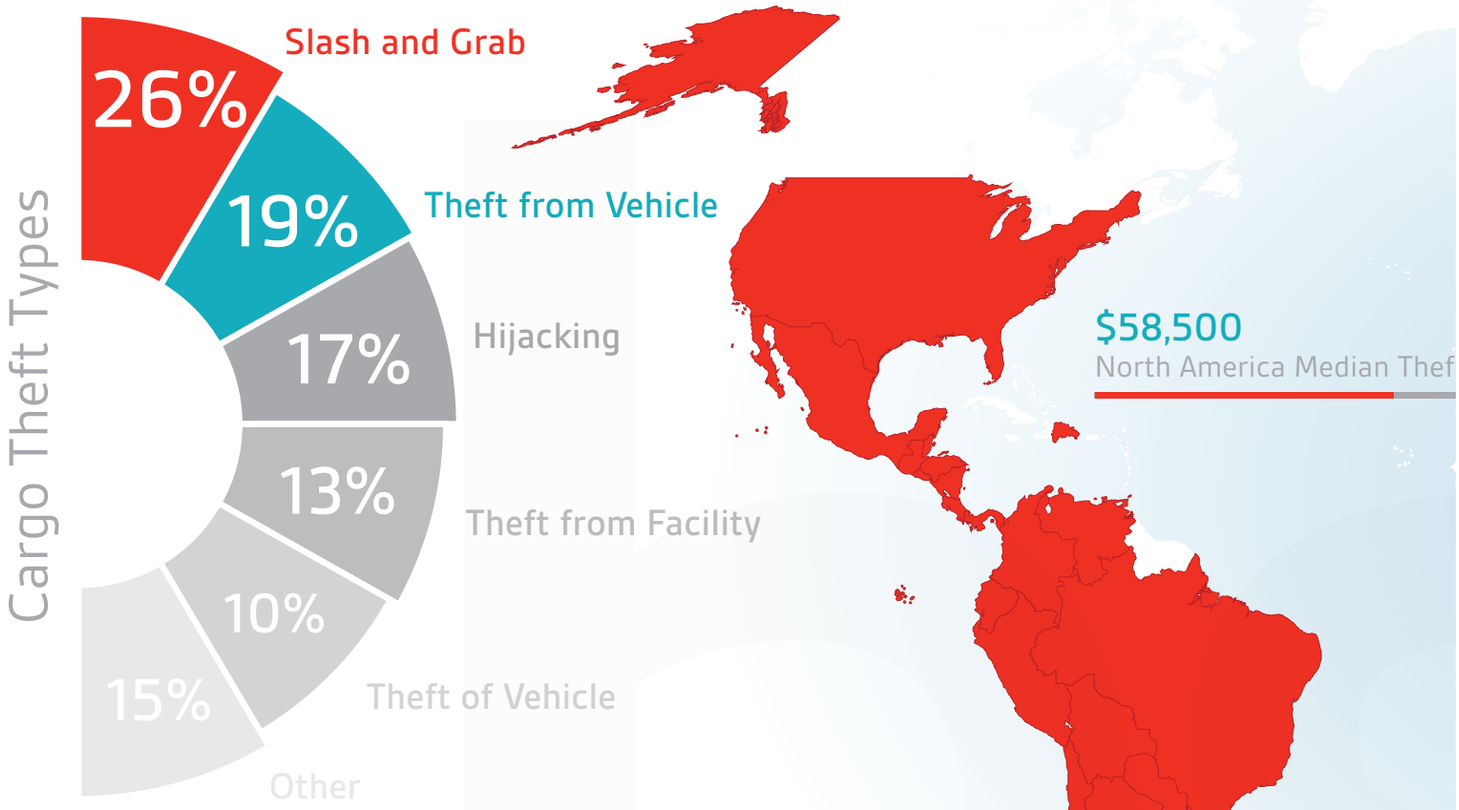


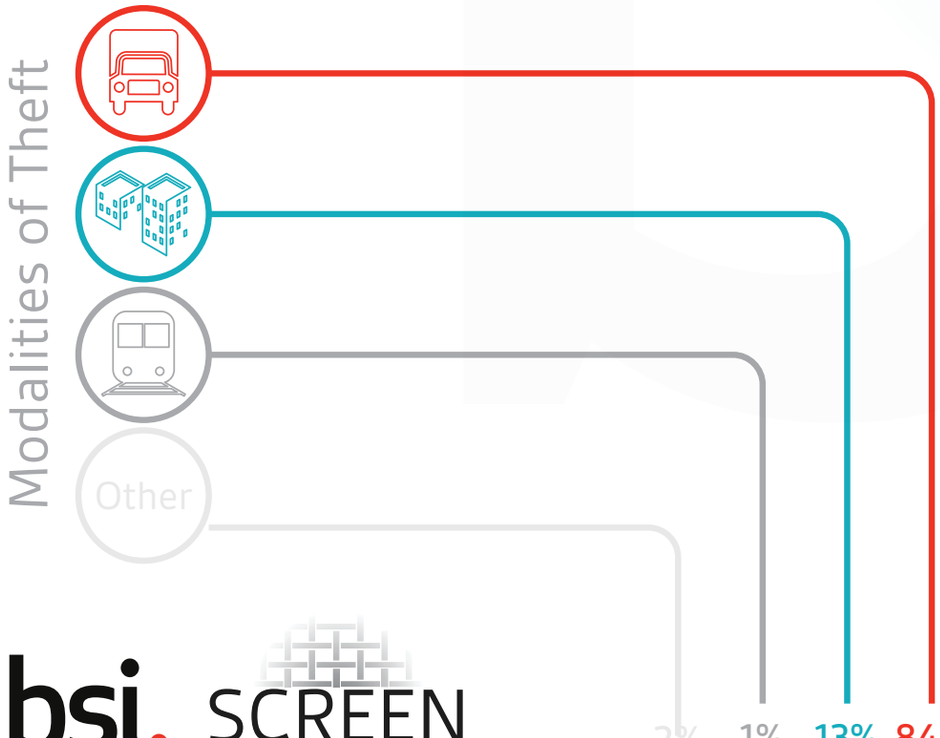
bsi.

SCREEN
Supply Chain Risk Exposure Evaluation Network

Global Cargo Theft Trends - 2018

Countries with hijackings in 2018





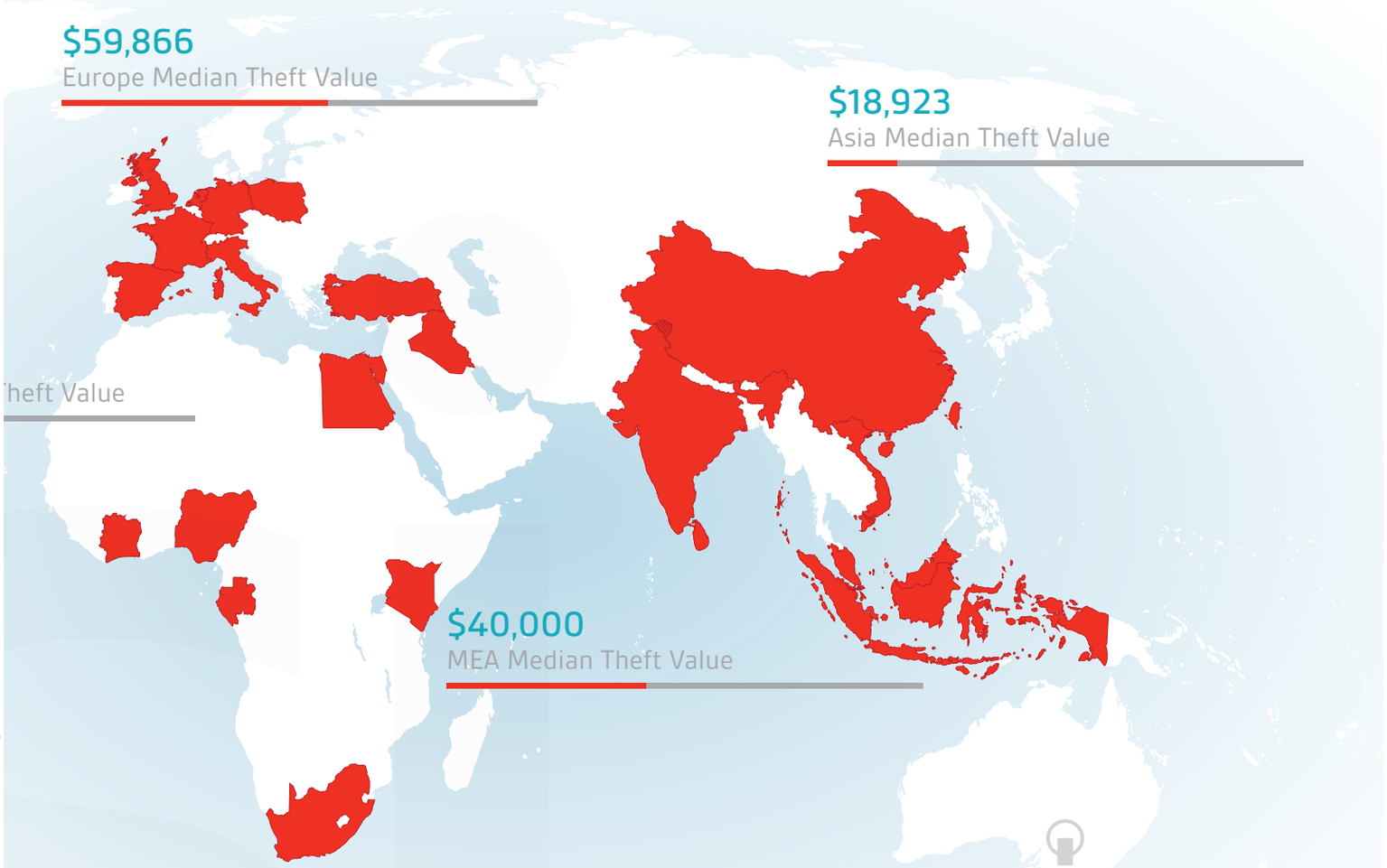
19%

Food and Beverage

bsi. SCREEN

Supply Chain Risk Exposure Evaluation Network

TT CLUB
50 years of established expertise



15
Per Day
Average number of cargo theft incidents

Top Commodities Stolen

15%
Alcohol and Tobacco

15%
Consumer Products

7%
Electronics

5%
Apparel and Footwear

39%
*Includes 14 other major types of commodities

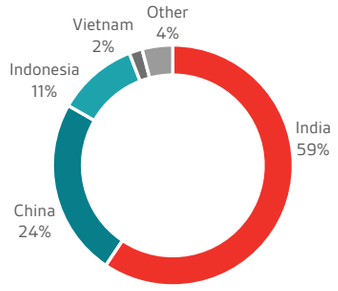
Asia

In Asia, BSI and TT Club most frequently recorded cargo thefts in India and China. Cargo thieves in these two countries are similar in profile and employ a wide-range of tactics. Methods range from very opportunistic means, such as pilferage and thefts by drivers, to more organized tactics, including in-transit truck thefts, where thieves drive a vehicle behind a moving cargo truck, board the vehicle, and then throw goods to trailing accomplices.

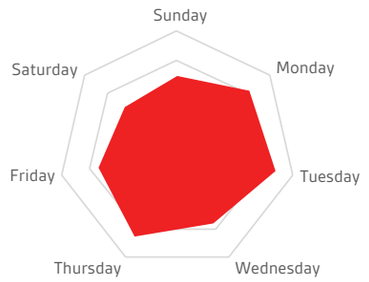
However, a significant portion of incidents involve thieves stealing goods directly from facilities in each of these countries. Supply chain corruption is a major element of thefts in China and India, with corrupt employees removing goods they are transporting or accessing shipments stored in warehouses or logistics facilities. Thieves generally pilfer small numbers of items but occasionally manage to steal larger quantities of goods. Other tactics include hijackings, slash-and-grab thefts, and counterweighting, where thieves remove goods and then use other items like rocks, sand, and water, to replace the weight of the stolen goods. In addition, poor access control protocols often contribute to the rate of cargo theft in Asia, with terminated employees often retaining facility keys that are then used to conduct thefts at a later date. BSI assesses that most recorded hijacking incidents in Asia occurred in India, with a significant number occurring in the northern portion of the country. Uttar Pradesh was a particularly notable hot spot for hijacking incidents.

Although Indonesia ranked third for total number of incidents recorded in 2018, BSI reduced the country's cargo theft rating due to an overall decrease in the frequency of incidents in the country. Despite this observed decrease in cargo theft risk, BSI continues to note that hijackings and the extortion of cargo truck drivers remain risks in Indonesia.

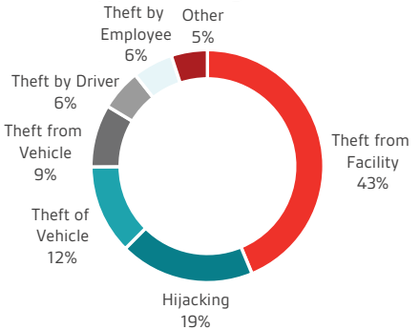
Top Countries for Cargo Theft



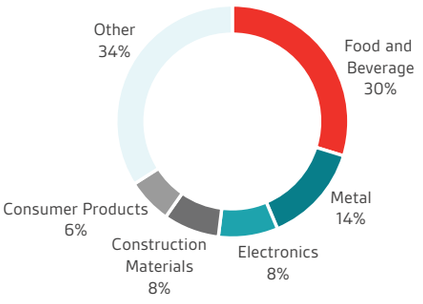
Cargo Theft by Day



Types of Cargo Theft



Top Commodities Stolen



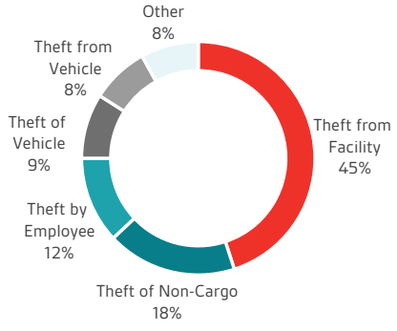
BSI Analysis: BSI Cargo Theft Data in China Highlights Insider Risk, Importance of Simple Security Protocols

February 8, 2019

Analysis of cargo theft incidents recorded by BSI in China last year continues to highlight the risk of thefts conducted by insiders and how relatively simple security protocols, such as parking in secure locations or ensuring proper access control procedures are being followed, can likely help mitigate the risk of most theft in the country. A significant percentage of incidents involve the theft of goods from facilities, often by current or former employees. In these incidents, BSI has noted that easily correctable security gaps, including ensuring doors remain secured or revoking access for terminated employees, likely could have prevented the majority of these incidents from occurring.

BSI has also identified the lack of secure parking options as a factor contributing to cargo truck thefts last year in China. The insecurity of expressway service areas propagates the vulnerability of cargo trucks, and often leads drivers to instead park in just-as-insecure roadside locations, exposing cargo shipments to opportunistic thieves. Utilizing team drivers to avoid stopping in insecure locations is one method that can help mitigate the risk of cargo truck thefts in China.

Types of Cargo Theft

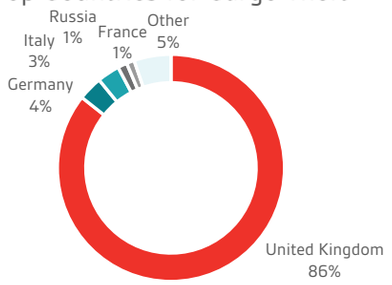


Europe

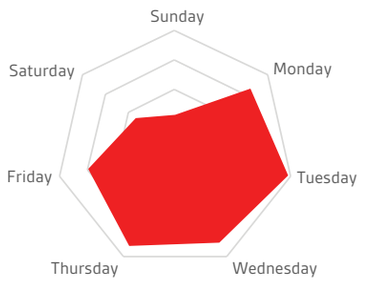
The lack of secure parking for cargo trucks is a major driver of cargo theft trends in Europe. All major countries of concern for cargo theft in the region, such as the United Kingdom and Germany, lack secure parking locations. Regulations that limit the length that cargo truck drivers can operate before taking a mandatory break also exacerbates the lack of secure parking and often forces drivers to stop in vulnerable locations.

This issue can also be seen in both the modality and types of cargo theft that BSI recorded in Europe, with thieves targeting trucks in most incidents. Thieves primarily relied on the slash-and-grab tactic, which accounted for nearly 50 percent of incidents. Thefts directly from truck trailers followed with approximately 20 percent of incidents. The high number of unsecured vehicles available for targeting helps explain the low number of facility thefts that BSI records in Europe. It is easier for thieves to target an unsecured cargo truck than it is to infiltrate and steal goods from often more-secured warehouses and other facilities. Furthermore, many parking sites in Europe lack security features to deter thieves from conducting thefts. The prevalence of soft-sided trailers in Europe also promulgates this trend and primarily explains the high frequency of the slash and grab tactic, in which thieves cut into the tarpaulin covering trailers to quickly remove goods. Additionally, thieves occasionally steal from unsecure trailers while drivers are delivering goods.

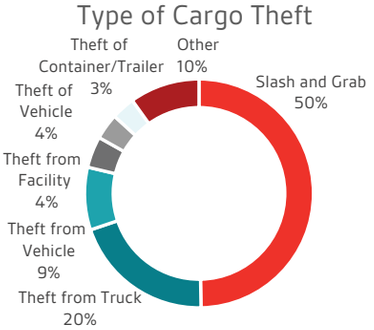
Top Countries for Cargo Theft



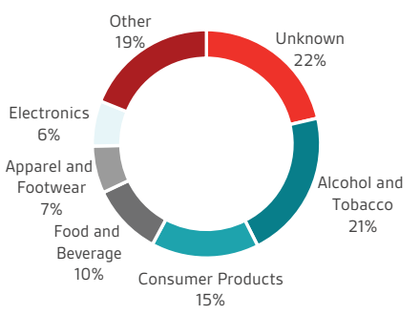
Cargo Theft by Day



Type of Cargo Theft



Top Commodities Stolen



BSI and TT Club frequently record slash and grab thefts throughout Europe. Although not as common of an occurrence in Europe as other regions in the world, namely South America, companies operating in certain countries in Europe should be aware of the potential for hijackings to occur. BSI most commonly records cargo truck hijackings in Italy, however, other countries in the region experience hijackings on occasion.

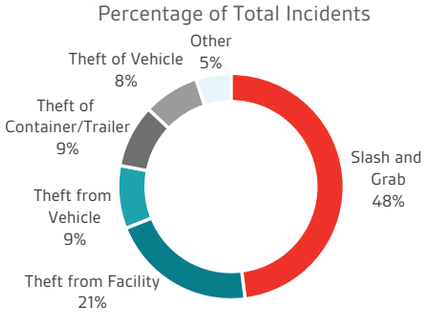
BSI Analysis: Thieves in Germany Most Often Utilize the Slash and Grab Tactic

January 25, 2019

According to BSI incident data, cargo thieves in Germany most often utilize the slash and grab tactic, which accounts for nearly half of all recorded incidents, while thefts from facilities account for 21 percent.

Cargo Theft in Germany by Type

Percentage of Total Incidents

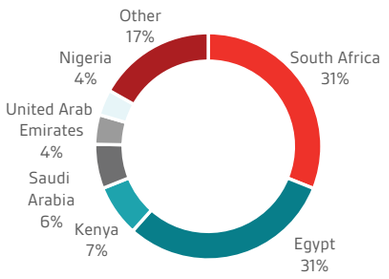


Middle East and Africa

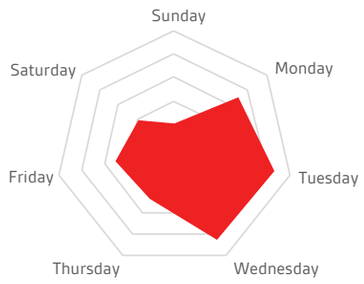
Unlike other regions in the world, BSI and TT Club most commonly recorded cargo truck hijackings as the primary type of theft in the Middle East and Africa. Poor security enforcement in most countries, combined with the widespread presence of weapons, enables thieves to conduct violent cargo truck hijackings with relative impunity. BSI most frequently recorded cargo truck hijackings in South Africa and Egypt in 2018.

Much like other regions in the world, supply chain corruption plays a key role in cargo theft in the Middle East and Africa. Cargo truck drivers may be forced to stop in unsecure locations at checkpoints established by corrupt officers demanding a bribe to pass, which places cargo shipments in a vulnerable situation. BSI also noted corrupt law enforcement officers facilitating thieves' use of police disguises in order to carry out cargo truck hijackings. While thieves are known to produce their own fake versions of uniforms or vehicles, some incidents involve thieves donning authentic police uniforms. Besides stealing the apparel, it is highly likely that in at least some of these instances, corrupt law enforcement officers provided the uniforms to thieves.

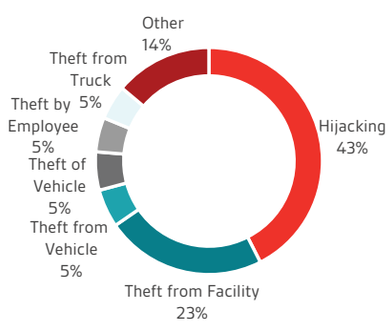
Top Countries for Cargo Theft



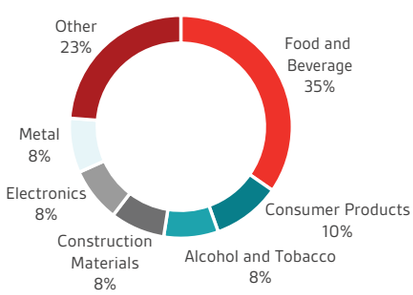
Cargo Theft by Day



Type of Cargo Theft



Top Commodities Stolen



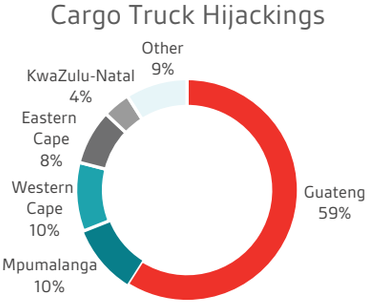
BSI and TT Club noted a spike in these types of thefts in South Africa during the first half of 2018. Known colloquially as "blue light" thefts, gangs in the country use fake police cars outfitted with police lights, emblems, and loudspeakers as well as wear uniforms that are potentially supplied by corrupt police officers. Some recommended security practices to mitigate this type of risk include training drivers to identify authentic police attire and vehicles and maintaining routine truck maintenance to ensure that drivers are not stopped for a supposedly broken taillight or other issue that a driver would know is non-existent.

South African Police Statistics Reveal Slight Increase in Cargo Truck Hijackings, Driven by Large Increase in Western Cape

September 12, 2018

BSI notes that new statistics released by the South African police for last year reveal a six percent increase in the number of cargo truck hijackings, driven primarily by a 109 percent increase in incidents in Western Cape over the previous year. Historically, BSI has noted cargo theft hijackings primarily in Gauteng Province, followed by KwaZulu-Natal, Mpumalanga, and Free State. In the last year, however, most cargo truck hijackings occurred in Guateng, Mpumalanga, Western Cape, and Eastern Cape, highlighting a significant drop in incidents in KwaZulu-Natal. Western Cape suffers from a high rate of gang-related activity, which has traditionally led to a high murder rate but could also help explain the spike in cargo truck hijackings that occurred in the province last year. A depleted police presence in the province also likely explains why cargo truck hijacking spiked.

Cargo Truck Hijackings



North America

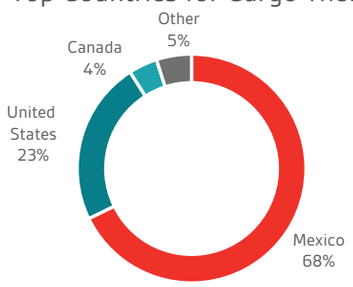
North America balances between two types of cargo theft, the more reserved thefts of unattended cargo trucks that BSI and TT Club record in the United States and Canada and the aggressive and often violent, hijackings characteristic of Mexico and the majority of Central America. Thieves in the United States and Canada most frequently steal unattended cargo trucks parked at unsecure locations, including truck stops and gas stations. Hijackings in these two countries are extremely rare.

In contrast, thieves in Mexico and Central America utilize cargo truck hijackings as a primary tactic. In most incidents that BSI records in this region, thieves often brandish, and occasionally use, firearms to force cargo truck drivers to the side of the road. Thieves commonly take drivers hostage during cargo truck hijackings, holding these personnel generally for a short period of time to delay police response.

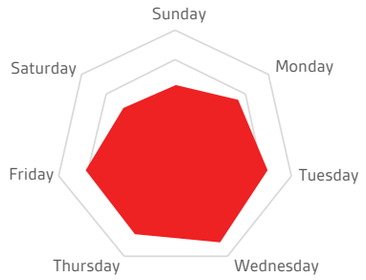
Thieves primarily stole food and beverage products, followed by consumer goods. BSI recorded the second greatest number of thefts of food and beverage shipments in North America, following Europe which had the most thefts of these products.

Thieves also conducted highly targeted thefts to steal pharmaceutical products, primarily targeting warehouses and delivery sites, as well as in-transit trucks, to steal various medicines.

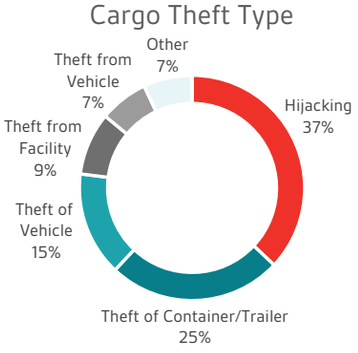
Top Countries for Cargo Theft



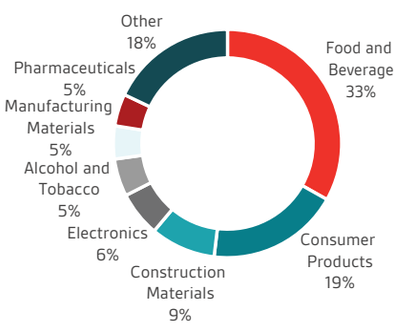
Cargo Theft by Day



Cargo Theft Type



Top Commodities Stolen

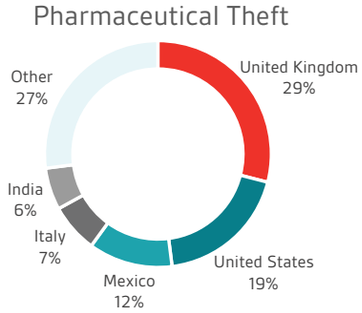


Trends in Pharmaceutical Cargo Theft

April 16, 2019

The pharmaceutical industry faces many supply chain-related challenges. Foremost, and most visible, is the outright theft of pharmaceuticals, typically while in transit. Based on available data, the top countries for pharmaceutical theft in 2018 were the United Kingdom, the United States, Mexico, Italy, and India. Thieves overwhelmingly strike the trucks moving pharmaceutical products globally, with the trucking modality targeted in almost three quarters of thefts recorded by BSI in 2018. The techniques involved in stealing pharmaceuticals vary, but the most common tactic is stealing from trucks by surreptitiously or overtly accessing the payload, a method which accounts for nearly one-third of thefts, followed by hijacking and theft from a facility.

Top Countries for Pharmaceutical Theft

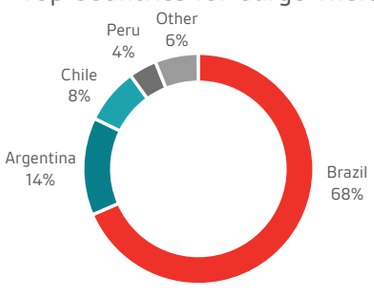


South America

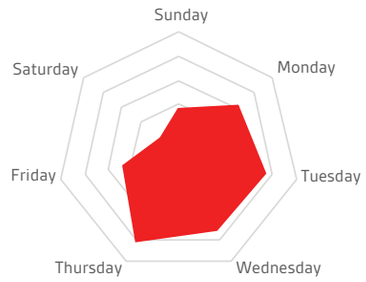
No other region in the world suffers from a higher rate of cargo truck hijackings than South America. BSI and TT Club recorded cargo truck hijackings in almost every country in the region during 2018, with thefts in Brazil accounting for the clear majority of collected incidents. The country continues to suffer from the highest rate of cargo truck hijackings in the world, with annual incident numbers totalling in the tens of thousands. Thieves occasionally steal goods from freight facilities and warehouses and target electronic shipments, as well as other goods such as food and beverage, automotive, and tobacco products.

One likely factor that explains the high rate of cargo theft in Brazil is the entrance of major gangs into the country's illegal drug trade and their need to finance such ventures. Local officials indicated that these gangs increasingly began to conduct cargo thefts to finance their illegal drug trafficking operations. The First Capital Gang (Primeiro Comando da Capital – PCC) is one such organized criminal group that BSI has identified as being tied to both cargo theft and illegal drug trafficking via cargo shipments. A lack of sufficient police resources and response almost certainly enabled the rate of cargo theft to expand in Brazil over the last several years, although a concerted effort by authorities in Rio de Janeiro last year likely helped lead to a slight decrease in overall cargo thefts in the state.

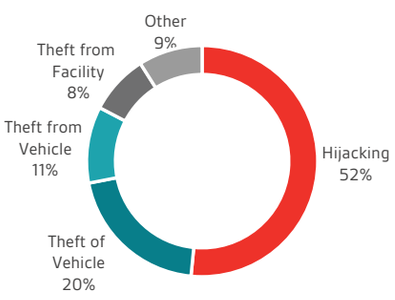
Top Countries for Cargo Theft



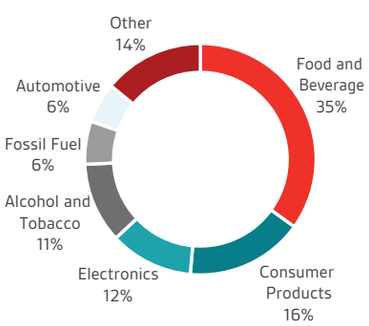
Cargo Theft by Day



Cargo Theft Type



Top Commodities Stolen



Other countries of concern for cargo theft in South America include Argentina, Chile, and Peru, all of which similarly suffer from high rates of cargo truck hijackings. Thieves primarily stole food and beverage products during hijacking incidents in these countries.

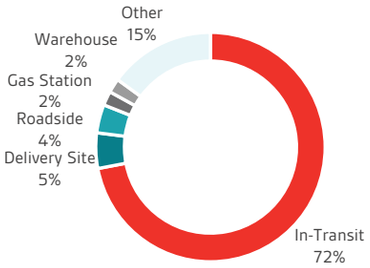
BSI Analysis: Thieves in Brazil Most Likely To Target Alcohol and Tobacco Shipments While In-Transit

February 1, 2019

Cargo thieves in Brazil most likely target alcohol and tobacco shipments while in-transit, according to BSI incident data. In-transit thefts account for well over half of total recorded incidents at 72 percent.

Cargo Theft in Brazil by Location

Percentage of Total Alcohol and Tobacco Incidents



Insider Threat

Introduction

Through analysis of available data BSI and TT Club have identified a common vulnerability – the Insider Threat.

People are an organisation's biggest asset; however, in some cases they can also pose an insider risk. As organisations implement increasingly sophisticated physical, procedural and cyber security measures to protect their assets from external threats, the recruitment of insiders becomes a more attractive option for those attempting to gain access.

The UK Government Centre for Protection of National Infrastructure (CPNI) defines an insider as "a person who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes".

An insider could be a full-time or part-time employee, a contractor or even a business partner. An insider could deliberately seek to join an organisation to conduct an insider act or may be triggered to act at some point during their employment. Employees may also inadvertently trigger security breaches through ignorance of rules, or deliberate non-compliance (due to pressure of work).

Official studies indicate that there are five main types of insider activity:

- unauthorised disclosure of sensitive information;
- process corruption;
- facilitation of third-party access to an organisation's assets;
- physical sabotage;
- and electronic or IT sabotage.

The most frequent types of insider activity identified were unauthorised disclosure of sensitive information (47%) and process corruption (42%). Noteworthy demographic information from the study indicated:

- Significantly more males engaged in insider activity (82%) than females (18%).
- 49% of insider cases occurred within the 31-45 years age category.
- Instances of insider cases increased with age until they peaked within this category and then decreased beyond 45 years of age.
- Most insider acts were carried out by permanent staff (88%); only 7% of cases involved contractors and only 5% involved agency or temporary staff.
- The duration of the insider activity ranged from less than six months (41%) to more than 5 years (11%).
- More than half of the cases were identified within the first year.
- 60% of cases were individuals who had worked for their organisation for less than 5 years.
- Most insider cases in the study were self-initiated (76%) rather than as a result of deliberate infiltration (6%); i.e. the individual saw an opportunity to exploit their access once they were employed rather than seeking employment with the intention of committing an insider act.

Financial gain was the single most common primary motivation (47%) and most closely linked to process corruption or giving access to assets. Organisations should develop effective strategies to assist in reducing the insider risk through the development of good management controls, including effective policies and procedures which seek to;

- Reduce the risk of recruiting staff who are likely to present a security concern
- Minimise the likelihood of existing employees becoming a security concern
- Reduce the risk of insider activity, protect the organisation's assets and, where necessary, carry out investigations to resolve suspicions or provide evidence for disciplinary procedures
- Implement security measures in a way that is proportionate to the risk

he document entitled Pre-Employment Screening: A Good Practice Guide, written by the Centre for the Protection of National Infra-structure, is a valuable resource for additional information.

Personnel Security - Recruiting and ongoing managing of staff

This section considers both mobile personnel (driver) and non-mobile personnel as both pose a potential security risk to your business. If they have been on-boarded with enough due diligence, full or part-time employees are arguably less of a security risk. Earning a regular salary should result in an increase in loyalty towards the employer and a reduced likelihood of theft risk.

Personnel Security - Pre-employment Screening

Pre-employment screening seeks to verify the credentials of job applicants and to check that they meet preconditions of employment (e.g. that they are legally permitted to take up an offer of employment). When conducting checks, it should be established whether the applicant has concealed important

information or otherwise misrepresented themselves. To this extent, pre-employment screening may be considered a test of character. The ways in which pre-employment screening is performed vary greatly between organisations. The aim of pre-employment screening is to obtain information about prospective or existing staff (if promoted and/or changing jobs in the organisation) and use that information to identify individuals who may present security concerns. Pre-employment screening is the foundation of good personnel security. It allows you to confirm the identity and credentials of those you are granting access to your sites and information and reduces the likelihood of an insider harming your business.

British Standard 7858 (BS7858) sets out recommendations for the security screening of individuals to be employed in an environment where the security and/or safety of people, services, personal data or property is a requirement of the employing organisation's operations or where such screening is in the public or corporate interest. The Standard is used widely in the private sector by organisations in their pre-employment screening processes, and by third-party screening companies undertaking pre-employment screening checks for organisations.

BS7858:2012 (version 4) comprises:

- proof of identity and address (wherever possible, supporting documentation should be photographic);
- details of education and employment;
- criminal records check;
- financial check; and
- checking of a character reference.

Initial screening of personnel is a vital component to any business's security management process. Effective screening satisfies several critical areas including confirmation that the person applying or presenting themselves to undertake a role is both qualified, capable, trustworthy and of good character.

It is clearly important to know that the person can undertake the required task, from a competency point of view, however just as important, if not more so, is to ensure from a security perspective you are able to verify that they are who they say they are. Many identity documents can easily be fraudulently doctored, and operators should develop a process which allows for only a small number of key official identity documents to be used, for example a current drivers' licence and a passport, that can be verified quickly and confidently through official channels.

At a minimum during pre-employment, screening operators should collect the following information that should, if the prospective candidate is subsequently hired, be regularly updated and maintained in an HR filing system:

- Home address
- Contact details, can these be verified?
- Proof of address and identity, utility bill?
- Copy of driving licence or operator's licence for machinery
- Emergency contact details
- Employment/character references for the last 5 years – have a process to follow these up
- Criminal record checks for any countries lived in, in the last 5 years
- Consider running a credit check

Personnel Security – Ongoing Screening

While pre-employment screening helps ensure that an organisation recruits trustworthy individuals, people and their circumstances and attitudes change, either gradually or in response to events. Studies indicate that over 75% of the insider acts were carried out by staff who had no malicious intent when joining the organisation, but whose loyalties changed after recruitment, in many circumstances the employee undertaking the insider act had been in their organisation for some years prior to undertaking the activity and exploited their access opportunistically. Some of the more common insider acts include:

- unauthorised disclosure of information
- process corruption
- stealing corporate information
- theft

Regular performance reviews should be undertaken. Whilst performance can obviously be more closely managed, it may be that a change in personal circumstances may be identified through such a process such as but not limited to;

- A change of relationship status
- A change of address
- A change in financial circumstances
- A change in their ability to perform their role (driving licence revoked)

The application of good ongoing personnel security principles adds huge value to physical and technical security measures in a cost-effective manner, promoting good leadership and management and maximising people as part of the security solution, including developing procedures and management controls related to;

- organisational security culture
- line management
- access controls
- secure contracting
- social engineering
- social networks and the use of the internet
- screening for the insider threat
- reporting concerns
- protective monitoring

- investigations
- exit procedures

Whilst the above applies to all personnel, security staff in particular could become vulnerable where circumstances have changed – could their integrity be compromised through a bribe for example?

Whilst our primary focus in this document is the risk of cargo theft, the identified principles should serve to highlight wider associated risks concerned with the theft of vehicles, trailers, chassis, containers, other CTUs, identity and fuel.

Where mobile personnel are concerned, in practice you are allowing them full trusted access to;

- A vehicle (and trailer/container) or a very valuable asset <US$100,000
- Valuable information about your business/your customer/ the cargo
- The cargo itself often <US$100,000
- Your businesses reputation (they will be representing you to your customer)

Personnel Security – Temporary Staff

In any business there will inevitably be periods of peak demand where temporary personnel are required and often at short notice. These occasions are ones where the diligent operator must have robust processes in place. Commercial and operational time pressures should not supersede the need to perform full due diligence checks, specifically checking to see if their employment has ever been terminated by a previous employer to understand the reasons why.

Where an employment agency is used, ensure that you fully understand and are satisfied with their due diligence procedures. What are they checking and how? Are they able to satisfy some of your requirements prior to the temporary worker arriving at your site?

What are the terms and conditions of the employment agency? Do they provide any liability cover if one of their temporary workers is either not capable of undertaking the task they are required to or causes loss through an act of negligence?

The document entitled Pre-Employment Screening: A Good Practice Guide, written by the Centre for the Protection of National Infrastructure, is a valuable resource for additional information.

Management controls

Clearly there exist specific critical areas of focus around recruitment where mitigation of this type of risk is concerned. Notwithstanding these, more general management controls also need to be considered. The risk emanating from everyday operational procedures may not be immediately identifiable; however, each breach of such management controls should be considered a near miss and could serve to weaken the entire security management program. Whilst not an exhaustive list some of the key controls and considerations are detailed below.

Access to customers' systems, premises and data

Do your employees have access to your customers' premises, systems or data? To what extent is access required and granted and on what basis? Does your customer have security requirements, are you able to adhere, manage and control these requirements for the personnel deployed?

Access to company uniform

It is often preferable to have both permanent and temporary personnel to be presented in company uniform. From a brand recognition and customer satisfaction perspective this can certainly be beneficial. Due consideration however should be given to control of the distribution of uniform. Could a temporary worker use the uniform to mis-represent themselves or others, posing as an employee of yours, allowing them access to premises, vehicles or cargo?

Access to ID badges

Identification badges are implemented as a means of security control. Badges can allow access to restricted areas for example. Strict controls need to be considered to monitor and manage the distribution of such badges. Are people able to use each other's badges? Do temporary personnel require a full access badge, or can their access be restricted?

Access to fuel/service cards

Fuel theft is a serious concern in many parts of the world. Many operators employ fuel and service cards which allow drivers to purchase fuel on credit on behalf of the company. These cards are very valuable assets to the operator and strict management controls must exist. Could the card be cloned or stolen and used illegitimately to purchase fuel or services? What restrictions are in place to prevent illegitimate use?

Where fuel is concerned, access to control or master keys for site critical infrastructure such as the fuel bunker is also of great importance.

Consider developing an anonymous reporting system. This will allow personnel to notify the operator of any security incidents, near misses or general concerns they may have. This source of information could be extremely valuable to the operator in better understanding the risks existing amongst the workforce.

Social Media and general communications

Social media is becoming an increasing, albeit less obvious, security threat. Especially amongst lone working mobile personnel social media is frequently used as a means of keeping in touch with friends, family and colleagues. All posts however are location sensitive and therefore traceable. For instance, a simple post by a mobile member of staff illustrating to colleagues where they are eating a meal, has the potential to divulge a series of valuable security data to organised criminals. Including the time, date and location, it of course also illustrates that the driver is away from their vehicle.

Non-mobile personnel are also susceptible to this type of risk and are also capable of unwittingly sharing valuable data from a given site. Bragging to friends for instance that they are unloading a container of high value cargo or the latest video game has the potential to raise awareness amongst the perpetrators of theft.

Whilst it may be challenging to restrict personnel from using social media platforms to communicate, operators should consider providing awareness training outlining the risks of the information being shared and how it might be used in the wrong hands.

More traditional methods of communication should also not be forgotten in this regard. Awareness training of all personnel should consider the risks of unwittingly divulging what could be valuable information to strangers. Conversations with peers about the cargo you are handling or carrying at any given time, or perhaps a regular collection from a certain site or delays experienced at a certain site can all be valuable to the organised criminal. Remember you don't know who might be listening to your conversation!

Operationally, information as to what cargo/load is in what trailer or container in the transport yard should be protected where possible. This information is obviously hugely valuable. Whilst it may be convenient to have these documents easily to hand in the dispatch office, you don't know who might be visiting and able to see this information. Nor do you know that their intentions are legitimate. This information and paperwork should be kept out of sight whenever possible.

Personnel Security - Instructions to staff

Instructions especially for temporary staff are a critical part of your on-boarding and security management procedure. Whilst generally it may be prudent to provide the minimum information possible to complete the task at hand, clear instructions are required regarding but not limited to;

- Routes
- Processes regarding documentation
- Processes and expectations regarding communications
- Company procedures regarding security

Provision of wider information including information around security should be avoided where possible. Information around the site CCTV coverage and usage for instance could be damaging. Information as to when security equipment is under maintenance or down time should be closely guarded. Any known weaknesses in terms of security (a damaged fence or an inoperable security gate) should also remain tightly guarded.

Information about the specification of the vehicles and equipment should also be closely guarded. For instance, the maintenance department unwittingly providing information about security technology fitted to vehicles could open vulnerabilities in the wrong hands. The location of items such as GPS tracking devices and their power source could be valuable to somebody with the intention of stealing a vehicle and cargo.

Where warehouse personnel are concerned, the risk profile changes slightly although many of the principles mentioned in other sections are applicable.

Consider to which areas of the facility it is critical for personnel to access. Can this be restricted?

The operational processes and protocols in place at any given location are likely to be slightly different and should also be appropriately managed in terms of communication to personnel. From a security perspective, is it critical for example that temporary personnel are inducted to every area of the facility or just to that area in which they are going to be working?

Knowledge of and access to cages within warehouse facilities storing high value or bonded cargoes should be severely restricted and where possible positioned away from external walls of the warehouse.

Where alarms are in place, the location of the control panel and alarm access codes should be closely managed. Codes for disarming alarms should be closely protected by persons with appropriate authority. An alarm system to which everybody knows the disarm code is not a secure one.

Periodic stock taking should always be undertaken by external independent personnel and audited accordingly.

Cargo arrival and dispatch information may appear to be low value data, however can prove extremely valuable to the perpetrators of theft. Divulging this type of information can result in perpetrators developing knowledge as to what cargo is loaded on which vehicles, when they are leaving site and the likely immediate route to be taken, affording them the opportunity to track and target cargo for theft.

Restricting information will prevent individuals developing a sound understanding of your operations and make it increasingly difficult for perpetrators to circumvent your security measures.

Where critical instructions are concerned, operators should consider potential language barriers. Where possible, pictorial instructions could be used to overcome certain challenges, however in the absence of any other practical options, then operators should strongly consider having instructions translated into several different applicable languages.

Consider access control, if security measures and access control systems exist, would it be better to chaperone temporary workers around the site rather than allowing them direct access?

Key controls

Develop key control policies for all vehicles. Key management where vehicles are concerned should be managed closely. Keys should not be left on, in or around vehicles at any time when the driver is not present. Vehicle keys should be signed in and out by somebody with the appropriate authority within the business. An appropriate identification and escalation process should be in place if keys are not returned when expected. A policy should also be in place for when a vehicle (and therefore keys) arrive back at site out of normal working hours. Vehicles should always be locked when the driver is not present.

Where there are duplicate ignition keys for certain vehicles, it would be prudent to ensure that only one key is ever in circulation with any spares locked away and under the direct control of management.

Petty theft

Incidents of petty theft can often be overlooked, it is often too much trouble to correctly handle such incidents versus the value of the commodity stolen. These incidents however should not be ignored. Such incidents should be treated seriously and with the appropriate severity in terms of employment status.

Persons conducting and getting away with petty theft will inevitably become greedy and their endeavours will escalate to a more serious problem. Setting and communicating clear expectations in this regard will reduce the risk of petty theft.

Recommendations

Develop and implement clear policies, management control procedures and include awareness training

Suggested critical considerations when developing policies, procedures and awareness;

- Implement layers of defence, starting with physical security, followed by clear management-level procedures and policies.
- Operate a least-privileged principle, where information and access are limited to a need-to-know basis.
- Employ a sound communication policy both internal and external considering the use of mobile devices and social media.
- Frequent awareness briefings and training programmes to educate all employees on best practice.
- Conduct comprehensive threat assessments to determine the threat landscape and understand the potential exposures.
- Risk assessment and risk treatment options can then be re-viewed and implemented to ensure a robust system is in place to prevent incidents where possible and equip employees to detect and respond in cases which could not be prevented.
- Vetting of third-party providers.

For more information, please contact us at **supplychain@bsigroup.com** or visit us at **bsi-supplychain.com**.

TT Club can be contacted at **riskmanagement@ttclub.com** or visit **www.ttclub.com**

SCREEN Intelligence

Supply Chain Risk Exposure Evaluation Network (SCREEN), is BSI's web-based, comprehensive global supply chain intelligence system. SCREEN is the most complete, publically available Supply Chain Security, Corporate Social Responsibility, and Business Continuity intelligence and analysis resource used to measure country level risk factors through BSI's 25 proprietary country level supply chain risk ratings. SCREEN's unique, proprietary global supply chain risk data and analysis helps organisations identify and understand where their supply chain risks exist. SCREEN generates trade interruption updates, BSI-authored special reports on major disruption incidents and trends, countermeasure programs, and risk mitigation best practices to help protect supply chains worldwide. SCREEN's intelligence provides organisations with full transparency of country risks and helps them to make intelligent risk-based decisions that drive resilience.

Interactive Risk Maps

Each proprietary risk indicator is conveniently displayed for over 200 countries through SCREEN's global risk mapping views. For every indicator, a country is assigned a rating of Low, Guarded, Elevated, High, or Severe. This rating system allows users to identify and categorize the threats to their supply chain and address them quickly.

Spotlight News

SCREEN's Spotlight News provides data and analysis on the most pressing global incidents on a daily basis. Each update encompasses a general summary of the incident and BSI's own analysis of the incident. The analysis provides the risk rating of the associated country and the explanation of the rating to help you better understand the country level threats and trends.

Automated Notifications

SCREEN provides users the ability to stay current and up to date with breaking news and changing conditions around the world that impact the integrity of their supply chain. Users are able to subscribe to the notifications for specific locations and subject areas that concern them the most.

Custom Report Builder

SCREEN's custom country report builder provides users with more control over the areas that are represented in the report. Users can easily pull and compare reports for multiple countries, threat assessments and commodities tagged throughout the SCREEN system instantly.

Additional Solutions and Services

Supplier Compliance Manager (SCM): BSI's automated self-assessment and audit analysis solution that quantifies and tracks supplier risk and compliance through various assessment methods to ensure your supply chain, brand and reputation are protected.

Training Services: Our customizable training services help develop a deeper understanding of supply chain security, corporate social responsibility and business continuity risks and how to quickly respond and proactively manage them.

Auditing Services: Our services provide organisations with complete visibility into their suppliers' practices and procedures worldwide. Our audits provide your organisation cost-effective assurance that your suppliers are not exposing your brand to risk.

Advisory Services: BSI's experienced risk management professionals leverage their knowledge and SCREEN intelligence to help organisations effectively identify, manage and mitigate risk and develop robust management programs.

4150 Drinkwater Blvd Ste 160, Scottsdale, AZ 85251
Tel: +1 480 421 5099
supplychain@bsigroup.com
bsigroup.com/supplychain