How Safe Are Your Shipments?

Theft, Risk, and the Steps You Can Take to Prioritize Loss Prevention

Purolator
Promises delivered™

Contents

Introduction

Introduction: The Impact of Freight and Theft

The stories continue to shock. Dozens of television sets stolen from a tractor-trailer parked outside a warehouse near Philadelphia, as the driver slept inside the cab. Jewelry and gemstones valued in the millions of dollars stolen from a parked truck, after the vehicle's two armed guards stopped off at a rest area. An organized crime ring broken up in the Greater Toronto Region, with the recovery of 28 containers of stolen cargo valued at $7 million. Increased reports of employee theft, fake trucking companies, and stolen identities of existing companies. The list goes on, and as the driver who had the television sets stolen told a local media outlet, "I've been driving for 20 years. I've never had this happen to me. Never ever."

The fact is, freight theft is big business. And the individuals responsible are more cunning, audacious—and successful—than ever before.

According to CargoNet theft prevention and recovery network, cargo theft across the United States and Canada increased by a shocking 57 percent during the second quarter of 2023, with much of the increase attributed to "shipment misdirection attacks," in which criminals use fraudulent truck company and logistics broker identities to misdirect freight. However, warehouses/distribution centers and parking lots remain the locations in which most thefts occur.

Further, CargoNet notes, "thieves stole over $44 million in shipments in the second quarter of 2023 and the average shipment value per event increased nearly $100,000 to $260,703 per theft." This increase, the company, which tracks cargo theft statistics across the U.S. and Canada, explains, is due to thieves increased propensity to focus on high value shipments.

While increased rates of theft and fraud are clearly concerning, the news is not all doom and gloom. That's because, just as bad actors have become more creative and daring in figuring out ways to steal and cheat, much has been accomplished to thwart those efforts. Law enforcement, security experts, private industry, and transportation and logistics professionals are at the forefront in developing new, more innovative ways to promote shipment safety. GPS trackers installed within freight loads, improved trailer locks, better warehouse yard lighting, real-time driver verification, improved carrier vetting and employee training, route optimization that minimizes downtime and shipment transfers, and IT network controls are among the security upgrades taking hold in today's supply chains.

Another critical factor is a business's choice of logistics provider. Logistics providers typically have a critical role in the supply chain that extends far beyond ensuring on-time shipment deliveries. Providers become deeply involved with their customers' businesses, and often have access to critical technology systems and shipment data, and identify the carrier that will transport each shipment. However, not every provider has invested in security upgrades, nor does every logistics company exercise precaution in taking steps to minimize shipment risk. At a time when criminals have become quite adept at identifying sub-par security systems and "easy marks," choosing a security-minded logistics partner should be a priority for all shippers.

The following discussion will provide an overview of current trends in shipment loss, including information about shipment types that are especially vulnerable. Critically important, the discussion will provide useful information about how businesses can protect their shipments, and how a qualified logistics provider can be integral to those efforts.

Supply Chains at Elevated Risk of Fraud and Theft, including Cyberattacks

Supply Chains at Elevated Risk of Fraud and Theft, including Cyberattacks

In a 2022 "Review of Cargo Crime," Roanoke Insurance Group, an international cargo insurance provider, warned that global supply chains faced "unprecedented risks," and cited several trends of particular concern, including:

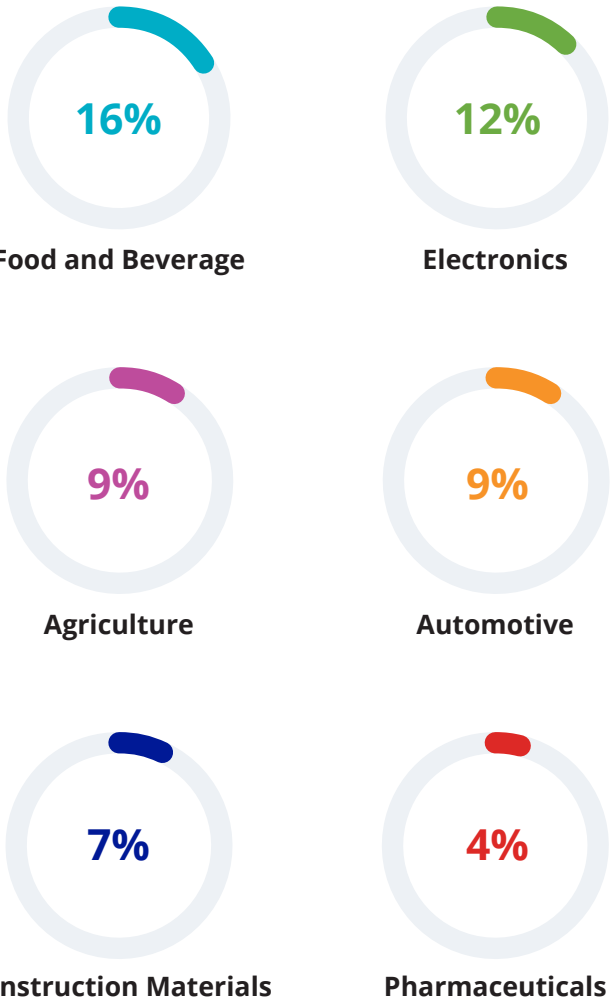
A continued decline in the global economy, in which higher living costs and employment uncertainty have helped foster demand for cheaper goods. "This economic shift indirectly incentivizes cargo theft, robbery, and burglary as criminals can steal essential or high-valued goods and sell them on the black market."

- **Cyber vulnerability and attacks.** Supply chains have been under tremendous strain in recent years, which has left them vulnerable to cyberattacks and other attempts at malfeasance. "Today's cargo thieves use sophisticated tactics and methods to execute their costly crimes," the analysis notes, with thieves using increasingly elaborate schemes to commit theft and "thwart efforts by law enforcement to catch them."
- **Rise in insider theft.** The report finds more than 20 percent "of all theft incidents recorded globally involved some form of insider participation." Insider theft includes an array of activities such as a warehouse door left unlocked, intentional sharing of a password, sharing information about security procedures or shipment information, staged hijackings, or outright lifting of inventory items.
- **Increase in facility/warehouse thefts.** Although most cargo is stolen directly from a truck, the report finds an alarming increase in warehouse thefts. This is likely due, the report notes, as a post-pandemic decrease in demand for goods has decreased the volume of goods being transported. "Because fewer cargo trucks transport goods, hijackings have decreased, but facility thefts have increased."

Overall, the report cites seven global leaders when it comes to cargo theft:

- India
- United States
- Brazil
- Russia
- Mexico
- Germany
- South Africa

The report also cites, on a global level, types of products most often stolen. That list includes:



Toronto, California, and Texas are Leading U.S. and Canadian Theft Locales

Closer to home, CargoNet which monitors cargo theft incidents in the United States and Canada, cites California, Texas, Florida, and Illinois as "most common" locations for full trailer thefts, with increased regional activity around New York City and Philadelphia. CargoNet notes that although burglaries of loaded vehicles actually decreased slightly last year, due largely to successful law enforcement initiatives, it remains a significant threat, "especially high-value shipments traveling on the I-40 corridor through Arizona, California, and New Mexico." The report also cites "significant growth in extortion and theft by conversion schemes," particularly from organized groups in Illinois and California.

In Canada, analysis by Roanoke cites Toronto as the "hotspot" for criminal activity, along other major transportation hubs including Montreal, Calgary, and Vancouver.

With regard to criminals' preferred methods, Roanoke notes that trucks are involved in 77 percent of U.S. cargo theft incidents, followed by facilities (21 percent), and rail (one percent).

Those numbers are similar in Canada, where trucks are involved in 80 percent of cargo theft incidents, followed by facilities (20 percent).

Worth noting, types of shipments prone to theft vary between the United States and Canada:

Shipment Type	Canada	United States
Electronics	NA	19%
Food and Beverage	36%	16%
Alcohol and Tobacco	12%	NA
Apparel and Footwear	12%	7%
Consumer Products	8%	16%
Machinery	8%	NA
Other	24%	35%

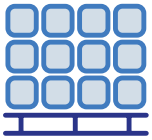
Source: Roanoke Insurance Group

Shipment Theft Comes in Many Forms

Unfortunately, cargo theft schemes have kept pace with technology, and can come in many forms, putting every step in the supply chain at risk. Travelers Insurance has identified five specific cargo theft "tactics," as a way to help shippers understand current risks. Those tactics include:

- Straight cargo theft
- Strategic cargo theft
- Technology
- Cyber
- Pilferage

In releasing this list, Traveler's Crime and Theft Specialist Scott Cornell noted: "There are some things about cargo theft that haven't changed very much over the years and there are many things that have changed significantly including new methods, targeted commodities, and the use of technology to commit cargo theft." Following is an overview of each tactic, along with discussion about how best to protect shipments.

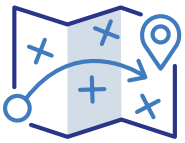


Straight Cargo Theft

This refers to "traditional" types of theft in which cargo is stolen from a stationery location. Common points of vulnerability include truck stops, parking lots, warehouse yards, roadside parking, and drop lots, among other venues in which cargo may be unattended.

Criminals have become increasingly brazen in their tactics. As referenced earlier, in May 2023 a napping driver awoke to find that thieves had cut a lock on his tractor-trailer and stolen 38 television sets. Travelers reports on criminals increasingly on the lookout for "temperatures on refrigerated trucks that indicate the presence of pharmaceutical loads, candy, or other types of desirable cargo."

Thieves are also taking advantage of warehouses which are increasingly chock full. "We're seeing an increase in break-ins at drop sites, as cargo tends to be at rest a lot longer than it previously would have been," said Tony Pelli, director of security and resilience at BSI supply chain risk consulting company in a 2022 Roanoke/BSI webinar. Pelli also noted increased reports of criminals following trucks out of facilities, and stealing loads at the first stop, which could be 100-200 miles away.



Strategic Cargo Theft

Travelers uses the "strategic" category to describe "theft that uses deceptive means." This type of theft, the insurer advises, is still evolving and refers to instances in which criminals use increasingly clever tactics to scam unsuspecting shippers. Thieves will stop at nothing in their efforts, with schemes that can include:

- **Fictitious Pickups.** Fictitious pickups occur when a driver arrives to pick up a shipment, claiming to represent a legitimate carrier when, in fact, the carrier is fraudulent. The shipper unknowingly releases its goods to the supposed carrier, only to learn its shipment has been stolen.

  One security expert, J.J. Coughlin of Southwest Transportation Security Council, speaking at a 2022 industry conference, highlighted the ease with which fictitious pickups occur. As reported by Transport Topics, Coughlin explained: "I can get on my computer right now and I can build a trucking company. Then I go on load boards and start bidding on loads. I get a load, then I go pick it up. I just take what they give me, and I just don't deliver it."

  Further, he noted, "a lot of times I can get five or six loads before they get onto me."

Coughlin cited one company in Southern California that had 11 loads stolen over the course of 10 days. The shipper thought it was dealing with four different carriers when in fact one single criminal was responsible for all 11 heists.

As Travelers points out, thieves take advantage of any and all opportunities to pounce when a shipper lets its guard down. This may include looking for loads brokered late on a Friday afternoon, or over a holiday, on the assumption that time constraints and deadlines will result in a less onerous vetting process.

According to CargoNet, fictitious pickup and fraud complaints were up 675 percent during the first 20 weeks of 2023 compared to the same period in 2022.

- **Identity Theft.** Roanoke refers to identity theft as a "more sophisticated" version of a fictitious pickup. This type of theft occurs when a criminal takes over the identity of a trucking company that has recently shut down. The fraudster uses the defunct company's DOT number and represents himself as a representative of that company. "We're seeing instances in which they're even slapping a logo on the side of the truck, so they aren't just pulling up in an unmarked truck," noted BIS's Tony Pelli.
- **Double-Brokering.** Truckstop load board provider defines double-brokering as the "unauthorized transfer of a load from one freight broker to another without the knowledge or consent of the shipper. It can be a result of negligence or poor communication, but in most cases, it's an act of malicious fraud."

  Truckstop notes that double-brokering complaints increased by 400 percent between Q4 2022 and Q1 2023. The practice is illegal and costs the freight industry over $100 million annually. There are two distinct types of double-brokering:

  - A legitimate carrier accepts a load for which it doesn't have capacity, and double-brokers the load without having the authority to do so. This is illegal, although there are often no claims unless an accident or damage occurs.
  - A broker gives a load to another broker. This occurs when a broker takes on more loads than it can handle, and transfers responsibility to another broker. The transfer is illegal, and is often made at a lower rate, with the original broker pocketing the difference.

  According to Transport Topics, double-brokering puts shipments at risk because of a loss of visibility and an increased risk of theft. The analysis cites Cassandra Gaines of Carrier Assure software company who explained that "brokers and shippers do not know who is actually in the custody of the goods. If something goes wrong, there is often no cargo insurance. Even worse, there is a higher risk of theft."

Technology

Travelers cites the increased use of technology to circumvent security protection initiatives. This includes, for example, the use of "sniffer" devices that detect GPS technology embedded within a trailer. Once a device is detected, the analysis notes, criminals "use a GPS jammer to block the technology so it can't be used to help law enforcement locate stolen goods." Another tactic is to place a stolen load in a parking lot and wait to see if law enforcement is able to determine its location.

Cyberattacks

TechTarget defines a cyberattack as "any attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage. Cyberattacks aim to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems."

Criminals have been able to successfully use cyberattacks to infiltrate shipping networks, especially as supply chains have become more automated. "Basic types of

cyberattacks are more commonly being used to aid in committing cargo theft," noted Traveler's Scott Cornell. "Businesses should prioritize protecting their online profiles using cybersecurity tools including antivirus software, two-factor authentication and other network defenses."

Specific types of cargo-related cyberattacks include:

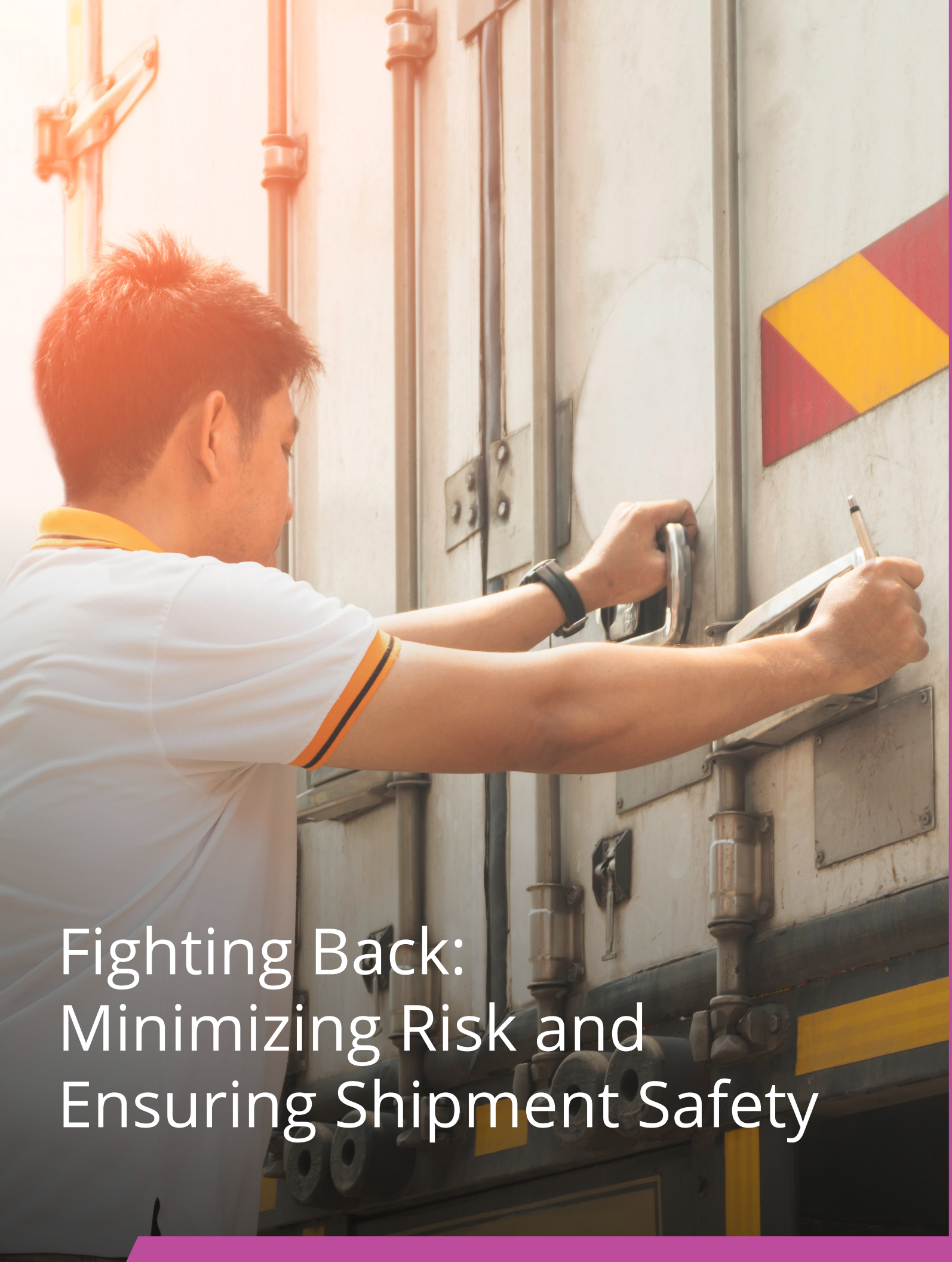
- **Phishing.** Phishing schemes refer to instances in which a criminal, pretending to be a carrier, reaches out to a business for payment, or who claims to want to remit payment. A link is sent to the unsuspecting victim, in an attempt to install malware that can infect a company's system and allow access to sensitive data. "Once you click on the link," explains BSI's Pelli, "they're able to steal identifying details about your company or another company with which you do business." Pelli said that instances of phishing are most often seen in Southern California, but it seems to be an "emerging trend" in Canada, especially in Western Canada.
- **Hacking/Password theft.** As mobile devices have become integral parts of the shipping process, so too have they become important access points for nefarious characters. By stealing passwords from mobile device users, criminals may gain unauthorized entry into a business's network which, reports Travelers, may provide hackers with access to pickup and delivery information. "Not only do these schemes put your company at greater risk for cargo theft, but they also leave your company vulnerable to regulatory fines and legal action."

Pilferage

Although thefts of full trailers tend to get more attention, Travelers notes that incidents of pilferage—thefts of partial shipments—are far more common. Pilferage tends to occur when a truck is left unattended in a rest area or parked in a yard. Or, as reported by Birds Eye Security, "in some cases, employees take items off trucks in the yard. They may then sneak them out of the property later, or they might leave them somewhere near an exit so that another set of criminals can come by later and pick them up."

There are several reasons why a criminal might prefer to steal a partial shipment:

- **Detection.** Since only part of a larger shipment is taken, a pilferage event is not always immediately noticed. "There's often a lag in detection that there's even been a theft," explains Traveler's Cornell, "because the drivers may not realize it until they reach the point of delivery, after making several stops along the route."
- **Less Risk.** Because pilferage often goes undetected, criminals are less likely to be caught. And, if they are caught, the consequences will likely be less severe than if an entire shipment had been lifted.
- **Fast Profits.** Pilfered items can often be quickly sold on a black market. This means fast profits for criminals, and a relatively quick way to rid themselves of the stolen merchandise.



Fighting Back: Minimizing Risk and Ensuring Shipment Safety

Fighting Back: Minimizing Risk and Ensuring Shipment Safety

As the above discussion makes clear, shipment theft comes in many forms, with varying degrees of sophistication. Shipments are vulnerable at every point in the supply chain, with criminals seeming to know no bounds when it comes to brazenness or ingenuity.

As serious as this threat is though, businesses can fight back with a few tricks of their own.

Security professionals have identified several "best practices" for helping businesses prioritize supply chain security. This includes recommendations for minimizing risk while shipments are in-transit or stored in a warehouse, and also for preventing technology-based security breaches that can lead to supply chain breakdowns. Following is an overview of several important recommendations.

Understand your vulnerabilities—Identify your Supply Chain Partners. A first step is to understand the points at which your shipments may be at risk, and this begins by identifying all parties who are either in a position to know about a planned shipment or will have a direct role in its execution. To do this, BSI's Pelli suggests mapping the complete chain of custody. "This includes any and all partners. Anyone who has control of freight at any point in time, or information about the freight," he suggests, noting increased incidences of insider information in helping to carry out thefts. "It's important to map not just the physical flow of goods, but the flow of information about those products as well," he added, suggesting that this information could be used to encourage supply chain partners to improve their focus on security.

Vet your carrier. Different trucking companies will have different security-focused practices in place, and not all ensure the highest levels of efficiency. But a little due diligence can help a shipper ensure its products are entrusted to a carrier that prioritizes security. Among the areas to consider, based on recommendations from Traveler's and Roanoke:

- **Verify the legitimacy of a company purporting to be a carrier.** A business should never assume that an individual arriving to pick up a shipment is, in fact, legitimate. Instead, Traveler's suggests, a business should "call the phone numbers on the company website and verify that people on the other end represent the legitimate carrier company you hired." Businesses should also verify a carrier's authenticity by checking with the Federal Motor Carrier Safety Administration (FMCSA) look up tool. Shippers can also check with local business organizations, or the applicable state's attorney general's office, or request—and document—a list of previous customers. Simple verification steps, which only take a few minutes, have helped stymie numerous fictitious pickups, double brokerage attempts and other bogus schemes.
- **Verify the identity of all drivers.** Businesses should implement a driver verification process as a best practice. This includes carefully examining and photographing each individual's driver's license, calling to verify affiliation with a listed trucking company, and maintaining a log that lists all driver names and truck numbers.

- **Review the security protocols in place for the carrier's fleet.** Extensive options are available to help keep cargo secure while loaded on a truck. Many of these features are relatively low-cost, but highly-effective. A listing provided by Western Truck Insurance Services includes:
  - Anti-theft devices including king pin locks, glad hand locks, air cuff locks, rear door locks, security cameras, and electronic fuel-line shutoff valves.
  - GPS tracking systems that generate an alarm to the carrier should a truck leave its scheduled route.
  - Options for team drivers as a way to keep shipments in motion and provide an extra body should a mid-transit stop be necessary.
- **Ask lots of questions.** A business should feel free to reach out to a carrier to ensure its commitment to security and internal protocols. A few questions to ask might include:
  - What types of training does the carrier have in place for drivers? Are drivers trained not to divulge information about their loads? Does the company offer basic security awareness training?
  - Will a driver be able to detect if he or she is being followed, and provided with a response protocol?
  - Does the carrier conduct background checks for new employees, and contact references?
  - What is the incident response protocol should a theft occur? What steps will be implemented to investigate, and what recourse will be provided should a business suffer a loss?
  - What about visibility? Is the carrier able to determine a shipment's precise location at any given time?
  - And what about chain of custody? Is the carrier able to identify every individual who comes in contact with the shipment?
  - Will your shipments be transferred from one carrier to another? If so, what protocols will be in place to minimize the risk of damage or theft? How long will your shipments be idle waiting for a hand off?

Vet your warehouses and other facilities. "A shipment at rest is a shipment at risk," is an oft-repeated mantra in the shipping industry. Indeed, with CargoNet listing warehouses/distribution centers and parking lots as the locations in which most thefts occur, businesses have reason to be concerned when shipments are not on the move. Both Travelers and Roanoke/BSI recommend a "layered approach" for ensuring warehouse security. "This doesn't necessarily have to be a high-tech solution or have to be very expensive," explains BSI's Tony Pelli. "The important thing is to make sure that there's more than just a fence, more than just access control," he added. Recommended "layers" include:

- Segmented controls that restrict access to different parts of the facility, and track individuals who come and go from each area.
- Closed circuit TVs and alarms.
- Strong, intact fence lines that encompass an entire parking/storage area.
  - All loads should have high-security seals that meet ISO-17712 standard requirements.
  - Parking facilities should be well-lit and continually surveilled.
- Regular security updates for all facility personnel.
- Tight management of contract security personnel.
- Regular IT system reviews to check for malware and other attempts to infiltrate warehouse systems. Hackers have become quite sophisticated in finding ways to intercept critical shipment information, often finding their way into a network via a phishing email, stolen password, or a password provided by a dishonest employee.

Control Dissemination of Shipment-Related information. In its webinar discussing shipment security, BSI security expert Tony Pelli cited a business that had experienced high rates of theft among shipments moving between the United States and Mexico. Specifically, shipments seemed to be most vulnerable in the short distance—three-to-four miles—between customs clearance at the airport and end-destination warehouses.

A review of logistics protocols determined that a lack of visibility among the carriers that transported the shipments was one contributing factor. But another "sticking point," Pelli noted, was the control of information between the customs broker and the carriers. "The customs broker would have all kinds of information and would send it out to everyone, whether or not they needed to have it," he said. Recipients of the critical shipment information, Pelli added, included "a bunch of people at the 3PL, at the carriers, and a bunch of people at the company that ran the factory." As a result, unsavory individuals were able to gain knowledge about shipment contents and travel plans, which was then transmitted to other criminals.

As this example makes clear, information should be restricted only to parties who truly have a need to know.

Guidance from Lodestar suggests that shippers can also help deter thefts by limiting information included on carton packaging. "Valuable shipment details should be limited to a need-to-know basis," notes Lodestar COO Jim Heide, writing in Transport Topics. "For example," he notes, "labeling a shipment of gold, 'gold,' could attract unwanted attention."

Prioritize Cybersecurity/Technology Security. As technology-based attacks become increasingly more numerous—and sophisticated—businesses need to be hyper-vigilant about protecting their technology systems and guarding against system disruptions. Travelers recommends implementing strong cyber security to help recognize and prevent efforts to infiltrate a network. The insurer advises companies to "closely examine their websites and the information they make available to the public." Potential causes of concern include references to specific customers or specific products, or listing detailed contact information for key employees, rather than providing a common point of contact.

The Best Defense is a Security-Focused Logistics Partner

The Best Defense is a Security-Focused Logistics Partner

Logistics providers, of course, have an integral role in businesses' supply chains, and can be a vital part of ensuring shipment security. The key though, is to enlist a logistics provider that prioritizes security, has extensive protocols in place with a documented record of success, and can also ensure first-rate logistics solutions that ensure on-time, seamless deliveries. A few security-related attributes to look for when selecting a logistics provider include:

- **Extensive in-network coverage.** Look for a provider that has the internal resources to ensure end-to-end in-network coverage. This avoids having to enlist external carriers and ensures chain of custody and accountability.
- **Minimal number of hand-offs and touches.** A high percentage of theft and damage occurs when shipments are transferred between facilities and vehicles. Chose a provider with the capacity to manage all supply chain functions including inventory, fulfillment, distribution, transit, and even returns. A single-source solution means fewer hands touching a shipment, and reduced opportunities for something to go awry.
- **Visibility and tracking.** Make sure a company can provide a high level of shipment visibility, including 24/7 tracking. A security-focused provider will always ensure real-time access to shipment whereabouts, which can be a tremendous source of peace of mind.
- **Scope of Services.** Look for a logistics provider that provides a selection of service levels that can accommodate different service needs—and prioritize security. A few options include:
  - **Mission Critical.** Shippers increasingly turn to expedited services, often referred to as "mission critical services," as an added layer of security for fragile, valuable, or time-sensitive shipments. As the name implies, mission critical services offer the highest levels of customer service, and ensure fast, guaranteed on-time deliveries. Shipments may travel via "next flight out," charter or expedited air service, via express ground solution, or a combination of air/freight services.

    Shipments benefit from reduced opportunities for theft since they are essentially in continual motion. The accelerated supply chain means fewer touches/hand-offs, which also reduces the risk for theft or damage. Shippers also benefit from high levels of visibility and accountability, as drivers maintain continual contact and provide regular updates. Additional security features may include on-board couriers, whereby an employee travels with an air shipment, and oversees its safe delivery to the end recipient.

- **Time-Definite.** Time-definite solutions allow shippers to know the precise day and timeframe of a shipment's arrival. Similar to expedited services, time-definite shipments also minimize the number of hand-offs and offer high degrees of visibility and accountability.

- **Alignment with International Security Standards.** The Transported Asset Protection Association (TAPA) is the agency responsible for developing internationally accepted supply chain standards to "tackle the multi-billion-dollar problem of cargo thefts from supply chains." TAPA recommendations extend far into the logistics process and set standards for warehouse/distribution center/yard security, fleet security, and cyber security. TAPA certification is regarded as the gold standard for logistics providers, carriers, and other providers, and demonstrates that a company is serious about loss prevention.

- **Membership in Trusted Trade Programs.** Another way to gauge a logistics provider's commitment to combatting theft is to determine its membership status in a government-authorized "trusted trade program." Such programs are usually voluntary joint government-business initiatives intended to ensure the safety of international shipments.

  In the United States, the Customs Trade Partnership Against Terrorism (CTPAT) program, managed by U.S. Customs and Border Protection (CBP), allows businesses to verify the security of their supply chains—and those of their vendors and suppliers—in exchange for favorable customs-related benefits. A similar program, Partners in Protection (PIP), is available in Canada through the Canada Border Services Agency (CBSA).

  Trusted trade programs require members to undergo an extensive certification process that requires detailed recordkeeping and on-site facility inspections. Membership is a good indication that a logistics provider not only prioritizes supply chain security but has demonstrated its commitment to government officials.

- **Experience matters!** Choose a logistics provider with an established record as a trusted, reputable company. Request information about the company's security record and ask to speak with current or past customers. And critically important, verify that the company has experience with your specific type of shipments. Technology companies and consumer electronics manufacturers, for example, are especially susceptible to theft, and will want to ensure that a potential partner has extensive protocols in place. If a company is reluctant to share this information, there may be a reason for this hesitancy.

Purolator—A Trusted Name in Security-Focused Logistics

Purolator is an example of a TAPA-certified logistics provider that prioritizes shipment security and loss prevention. The company is a leading provider of logistics services for shipments moving between and within the United States and Canada.

In Canada, Purolator Inc. maintains an extensive distribution network that ensures access to all provinces and territories, with the ability to reach an impressive 99.5 percent of all postal codes. The company's U.S. subsidiary, Purolator International leverages its non-asset-based network to build innovative, highly-flexible solutions that address businesses' unique needs. Together, the Purolator companies provide comprehensive coverage throughout the United States and Canada with an undeterred focus on shipment protection and security. The company's security-based attributes include:

- **Investment in experienced security personnel.** Purolator maintains a team of internal employees who spend 100 percent of their time focused on shipment security. Team members collectively have decades of experience working in law enforcement, cybersecurity, logistics and related fields. The team focuses its efforts on monitoring shipments for irregular activity, analyzing data, collaborating with industry security professionals, and ensuring that proper controls and practices are in place to maximize shipment security.

- **Investment in fleet and facility security.** Purolator ensures state-of-the-art security practices throughout its network of assets. All trucks, vans, planes, warehouses, processing facilities, service centers and other assets meet or exceed TAPA security guidance. This includes widespread use of cameras, thermal imagery, radar, communication networks, locking systems, and extensive employee training and vetting.
- **Comprehensive supply chain services.** Purolator offers complete supply chain management which ensures a high degree of accountability and visibility, and limits the number of parties with access to shipment information. With Purolator responsible for all aspects of the logistics process, shipments move seamlessly through the process via a highly-secure technology network, handled by security-trained employees, and ultimately delivered by uniformed personnel who have been vetted and verified.
- **Extensive distribution network and geographic reach.** Few logistics companies offer extensive services in both the U.S. and Canadian markets. In Canada, most carriers only service certain geographic regions. This often results in businesses enlisting a U.S. company to transport shipments to the border, which are then transferred to one of several regional Canadian companies for end-deliveries throughout Canada. A company with customers located across Canada could easily find itself with a network of a dozen or so regional carriers. Such a solution is rife with inefficiency, and with a large number of parties involved in the distribution process, exposes shipments to an increased risk of damage or theft.
  - Purolator is different. In the United States, Purolator International draws from its extensive network of carriers to identify the ideal solution for each customer. This allows businesses to better manage their facility schedules, and avoids instances of shipments piling up, waiting for a pickup that doesn't quite match up with its production schedule. Instead, Purolator customizes a pickup schedule to meet a business's precise needs. This includes the ability to collect freight and parcel shipments via the same truck, eliminating the expense and inefficiency of a second pickup.
  - Once in the Purolator network, shipments are routed for direct transit to the Canadian border, many times arriving on the same day. This seamless service means shipments undergo a minimal number of touches, which dramatically reduces opportunity for damage or theft.
  - After crossing the border, shipments continue within the Purolator network. Courier shipments are quickly loaded for delivery via the company's extensive courier network. Larger shipments enter the company's LTL/Freight network for similar direct deliveries.
  - The scope of Purolator's network eliminates the need to enlist multiple carriers. Instead, shipments remain within Purolator's control, which minimizes the number of hand-offs, and reduces the risk of damage or theft.
- **Trusted Trade Program participation.** Purolator is an active participant in the U.S. Customs Trade Partnership Against Terrorism program, and Canada's Partners in Protection supply chain security program. Purolator is also a certified member of the Transported Asset Protection Association (TAPA).

Shipment Security Checklist

Shipment Security Checklist

Enlisting a security-focused logistics partner should be a priority for all businesses. But this is just one of many steps that will provide overall supply chain protection. The Transported Asset Protection Association (TAPA) has established standards to help businesses reduce their vulnerability to theft and improve overall supply chain security. A sampling of TAPA-suggested best practices includes:

Verify everything. Check the credentials of any individual claiming to represent a certain logistics or trucking company. Do not rely on the contact information listed on an individual's business card but instead, use the phone number listed on the company's website. In addition, also verify:

- That the trucking company itself is legitimate.
- The legitimacy of the company's website.
- That the phone number listed for the company is authentic.

Require advance truck and driver information. When possible, require that a trucking company provide you with advance information about the truck and driver scheduled to arrive at your facility. This includes a driver's name and photo, trailer number and license plate, and specific time of arrival.

- Once the driver arrives, confirm that his/her ID is current and that the photo matches the individual standing in front of you. Make a copy/take a photo of the ID, if allowed.

Vet your staff. Conduct stringent employee background checks and verify references. Be sure to retrieve all credentials and discontinue network access when an employee leaves your company.

Train your staff. Training should be an ongoing endeavor for your company. Your staff is a critical first line of defense in helping to prevent theft. Train employees to be on guard for suspicious behaviors, and telltale signs when a truck is being followed. Ensure that all employees know the process for elevating instances of suspicious behavior.

Secure your facility. Install cameras and CCTV surveillance, ensure storage and loading areas are well lit and securely locked. Limit access to storage areas and maintain activity logs. Install GPS tracking on all company vehicles and place tracking monitors within shipments.

Conduct Regular IT System Cleanups. Protect your computer network with regular scans to detect malware, hack attempts, and Trojan horses. Be sure employees understand the importance of network security and know how to detect phishing schemes and can protect their passwords and log-on credentials.

Conclusion

Conclusion

An August 2023 article in *The Wall Street Journal* highlighted the growing appeal of Nike sneakers to criminals, who have built a lucrative black market to quickly resell stolen goods. "Nike goods have been stolen at almost every step of the supply chain, from distribution centers, rail yards and storage trains to FedEx delivery trucks," the article noted, "highlighting how retail crime goes beyond shoplifting or smash-and-grab thefts in stores."

As it turns out, just a few weeks before that article was published, more than $3 million in stolen Nike products were found in a Los Angeles-area warehouse. Included in the heist, the *Journal* reported, "were pairs of an unreleased style of the NOCTA x Nike Glide, a $160 sneaker collaboration between the sportwear giant and hip-hop superstar Drake." A few weeks before that, a crime ring was broken up, also in Los Angeles, which involved the theft of roughly $750,000 in Nike merchandise.

The article pointed out the sophisticated techniques criminals are using to identify shipments and pull off heists. "Organized retail crime groups carry out carefully planned operations. They learn about store layouts, and they create lists of valuable inventory at each location. Criminals also enlist spotters trained to analyze contents of shipping containers based on bill of lading information, retail and logistics company employees who collude with criminal groups, fraudulent trucking companies, and abuse load board postings.

One cargo security expert summed up the situation by noting: "The good guys, us, we're playing checkers, and the bad guys are playing chess. They're always one or two steps ahead of us."

Clearly, shipment security should be a top priority for all U.S. businesses. A critical first step is to understand the enormity of the problem and recognize that all shipments are at risk. From there, a business can fight back by implementing solid security protocols across its supply chain. With a few commonsense changes, businesses can protect their assets and send the message that when it comes to shipment theft, the good guys will ultimately prevail.

Find out how Purolator can help prioritize your loss prevention.

Contact us

Purolator
Promises delivered™

purolator.com