CROSS-BORDER MONITORING & RESPONSE SERVICES FOR SECURE SUPPLY CHAIN TRANSPORTATION

CONTENTS

INTRODUCTION

Product thefts from supply chains in Europe, the Middle East and Africa (EMEA) in 2020 produced losses of more than €172 million, according to the Transported Asset Protection Association's (TAPA) Cargo Theft Annual Report.

This despite most of the region being in lockdown as nations took drastic steps to prevent the spread of coronavirus.

Some key statistics from the report that show the extent of the loss are included below:

At G4S, we believe products should move from production to end the consumer **seamlessly,** without facing any security issues.

Our Secure Supply Chain solutions ensure the **identification, assessment** and **prioritisation** of efforts needed to manage potential threats and risks.

This requires a **multi-faceted** approach to protecting the checkpoints, assets and infrastructure involved with the production and transportation of your products and services.

This whitepaper acknowledges many of the challenges and risks we see every day in the international supply chain industry and identifies how we at G4S address them.

THE CROSS-BORDER TRANSPORTATION CHALLENGE

Supply chain managers must fight the financial losses, customer dissatisfaction and reputational damage that results in delays or loss to assets in transit.

Not only do they need to protect their assets from theft, but also from damage and contamination — all while assets are in transit, at factories and in warehouses waiting for shipment.

Supply chains in the current global marketplace operate with small margins and need to be tightly controlled to meet supply, satisfy demand and ensure profitability.

Given the sensitivities and complexities involved, supply chains are uniquely more vulnerable to security risks than standalone businesses. These issues can wreak havoc, yet are commonly overlooked.

Let's start by exploring some of the challenges that present themselves along the way.

Prior to Shipment

The challenge starts from the production line to warehouse and distribution hub. Across the world, issues such as employee theft and product damage cost retailers and wholesalers billions of dollars every year.

Staff Theft

It's sometimes difficult for employers to acknowledge, but staff theft can be responsible for significant losses in the logistics sectors.

Whether it be poverty and/or financial difficulty, staff may take items which can be resold to help pay bills, or because an item is unaffordable for them. With increasing levels of unemployment and redundancies, there's a risk that more staff may steal from their workplace to help cope with a lower household income.

For some employees, stealing is a way of getting back at a company or boss they feel has wronged them. Whether they feel overworked, unmotivated at work or taken advantage of – low staff morale can be costly to a business as some employees seek to redress the balance in their own way.

Crime is often opportunistic, and if an employee feels there is an opportunity to commit a crime, they are more likely to do so. In other cases, employees who normally wouldn't steal can become tempted when they hear rumours of other colleagues getting away with it. Some employees will even justify their actions with the belief that the theft will be covered by insurance, that item(s) won't be missed, or that the company is big enough – or rich enough – to absorb the loss.

Thefts can range from very small, low cost items, through to high-value products that are resold online.

Inventory Fraud

Inventory fraud involves the theft of physical inventory items and the misstatement of inventory records on a company's financial statements. Inventory consists of raw materials, unfinished and finished goods that are generally stored in warehouses. Timely fraud detection using fit for purpose systems and processes can save significant time and money.

Organised Crime

Organised crime is planned and co-ordinated criminal behaviour, conducted by people working together on a continuing basis. Motivation is often, but not always, financial gain. Organised crime in this and other countries recognises neither national borders nor national interests.

Organised crime in the United Kingdom (UK) costs in excess of £24 billion each year.

Among identified trends apparent during the recent lockdowns has been a move away from the theft of higher value, more easily traced goods, such as electronics and domestic appliances, to food and drink commodities.

Thieves have also noted and exploited the congestion in the supply chain that has increased the use of temporary warehousing and storage sites which are not always as secure as established premises.

Deceptive Pickups

This type of cargo theft can involve unconventional methods, including the use of fraud and deceptive information intended to trick shippers, brokers and carriers to give the load to the thieves instead of the legitimate carrier.

Trends include identity theft, fictitious pick-ups, double brokering scams and fraudulent carriers as well as hybrid combinations of these methods used together to create even more confusion. Cargo thieves often look for loads being brokered late in the afternoon on Fridays in hopes that time constraints and deadlines will lend to mistakes and less stringent vetting of the carrier.

To avoid becoming a victim of strategic cargo theft, companies must employ strategies that will ensure consistent and thorough vetting practices of all carriers.

Don't forget safety

Warehouses are generally large spaces tightly packed with stored goods - meaning even a small fire can be devastating. Aside from the obvious issue of extensive product damage from the flames and heat, there may be smoke damage, employee injury, or forced relocation to a new warehouse.

Flooding is also a common warehouse risk, especially in areas prone to natural disasters and high water levels. A high percentage of inventory stored in warehouses is susceptible to water damage.

All organisations have a responsibility to ensure that they're handling environmentally hazardous substances correctly. Dangerous materials can easily cause supply chain delays or damage valuable stock.

Aside from damages from fire, flood, and the like, warehouse inventory can also be damaged from its time in the facility. The following precautions should be considered by staff:

- Ensure the facility uses proper storage techniques for each type of good. The temperature of the warehouse and amount of weight placed on top of an item are particularly important.
- In addition to natural hazards, due to their high volume of inventory, warehouses and distribution centres are often at high risk for burglary and theft, especially if inventory is high-value
- Valid risk assessments need to be undertaken to ensure adequate deterrent such as physical security (fences or barriers) or a visible presence such as security officers with canine.
- In addition to the deterrent, it is critical to detect unauthorised access in real time. Therefore, fit for purpose surveillance should proactively highlight unusual or suspicious activity in order to take preventative action.

Asset Location

TAPA research highlights that over €172 million of products were stolen from supply chains in EMEA in 2020.

Therefore, throughout the manufacturing and delivery process, assets, whether the materials to create a product or the final product itself, need to be traceable. Higher value assets should ideally be traceable in real time.

Tracking by default is based on a single GPS device providing the latest known position of the asset. Fleet managers need to be well familiar with the technology to interpret correctly the information collected. In this case all kinds of questions arise:

- Is the information provided live or logged due to loss of communication?
- Is the position on the map the actual position or, due to a lack of GPS coverage, is this the nearest GSM (Global System for Mobile Communications) antenna, placing the vehicle in an area of a few square kilometers?
- Is the device working correctly during a route or is it malfunctioning and they'll find out the hard way?
- Can they make business decisions that could have an impact on the buyer's cargo with this type of information?

New digital advances like the convergence of the Internet of Things with artificial intelligence (AI) and blockchain mean you can now communicate multiple characteristics of an asset. These include the position, status and quantifiable data like temperature, speed and provenance.

However, tracking will only get you so far - monitoring is where you should be targeting

This means knowing where your vehicle and cargo should be and performing validation checks compared to where you see them - using multiple sources of information on a single screen within the same environment.

Monitoring is to apply complex business rules to filter out the "noise" and provide to the users only the information they need to see, applying automation to avoid human mistakes and missed alarms, and building consolidated reports.

When an incident is initiated - and it will happen frequently as TAPA EMEA's IncidentInformation Service (IIS) statistics have proved - monitoring should have the agreed, per customer/per type of route, response protocols in the system in order for theoperators to instantly activate the process in simple steps.

Given that so much transportation takes place on cross-border routes, an incident in a different country with language barriers makes the exercise even more difficult.

Exchanging information through emails to keep track of the status during a criticalincident has been proven inefficient. Thus, monitoring today requires a common platform across the network of countries and response teams, having full visibility of the incident information, the current status and the steps required for every single customer.

[1] **https://tapaemea.org/assets/downloads/PRESS-RELEASE-Over-%E2%82%AC172-million-of-products-stolen-from-supply-chains-in-EMEA-in-2020.pdf**

Costs through Avoidable Delays

Vehicles are equally important. Without vehicle tracking, it's extremely difficult to see the route your drivers are taking. There may be problem areas and patterns that can emerge with the kind of data fleet tracking systems can provide. Is there a particular route that gets slowed down at the same time every day?

Knowing this kind of information can allow you to improve the efficiency of your drivers' journeys.

Stopping in High Risk Areas

With criminals becoming more sophisticated, it is so important that unscheduled stops are avoided wherever possible. Unscheduled stops in unsecure locations with undefined perimeters and poor visibility provide the ideal opportunity for criminals to execute an attack.

Only effective monitoring will provide real time location intelligence before it is too late.

Maintaining Standards

Whether we're talking about aptitude or attitude, tracking and monitoring solutions allow you to determine which of your drivers are and aren't operating at the standard you expect.

This will also allow you to accurately assess your drivers, so you can incentivise good driving and reward your best drivers. It will also allow you to determine where additional training may be required.

Preparing for a Crisis

Ranging from a major accident on a main road to an unexpected extreme weather event, a crisis can put both your drivers and your vehicles in danger. Fleet tracking allows you to quickly know if you have any assets in an affected area, giving you both peace of mind and the ability to take action if necessary.

Whilst delays are costly and inconvenient, a safety event (like a vehicle accident or engine break down in a remote area) can easily turn into a more serious security incident (imagine a driver is injured and picked up by ambulance) - leaving cargo unattended.

In these situations, costs resulting from delays are worsened through material losses causing significant financial and reputational damage.

THE CROSS-BORDER TRANSPORTATION CHALLENGE

Theft or Loss in transit

Research by supply chain intelligence provider BSI shows that theft of cargo in transit remained over 70% of all supply chain theft. Therefore, ensuring vehicles are secured and are monitored in real time will help with early warning and problem identification.

Don't forget your people

It is critical to not neglect your duty of care to those working in the supply chain. It is important to retain two way communication on a 24*7 basis around the clock to ensure permanent dialogue and allowing security to intervene as and when necessary.

Cross Border Response

It is also critical to consider how to organise a physical response when necessary when operating cross border. Real time two way communication is important but it falls down if you have no response capability when it is needed.

START WITH A RISK-BASED APPROACH

We adopt a consultative, risk-based approach which ends with the best possible combination of people, professional and data and technology services to suit your risks but it begins with a thorough evaluation of:-

- What you are looking to protect
- What you are looking to protect it from
- How best to protect it

Whilst many of our customers would claim to already understand these dynamics, we will provide a detailed gap analysis, adopting the market standards (like TAPA) to evaluate the customers security level and provide recommendations for enhancements.

In these situations, it is our role to illustrate our understanding of these standards. recommendations for improvements and then highlight proposals for the best possible integrated security solution.

THE THREE PILLARS OF SECURING CROSS-BORDER TRANSPORTATION

We break our offering into three distinct categories outlined below.

Category 1: Fleet

This involves real time fleet monitoring, availability management and location of your vehicles internationally at any time.

Category 2: Assets

Securing and preventing damage to or loss of assets whilst in stock or in transit.

Category 3: People

Meeting your duty of care by protecting your staff from the risks that present themselves during cross-border travel.

WHAT DO YOU NEED TO PROTECT FROM?

The first priority has to be to prevent putting your staff in danger and meeting your employee duty of care to ensure that if and when an incident occurs, a suitable system or process is in place to assist.

Expensive cargo or assets will be a key target for many of the areas that we have highlighted elsewhere in this document including:-

- Insider theft
- Organised crime
- Fraud

And many more.

It is really the consequences of any combination of these that should remain at the forefront of planning,whether it be:-

- Financial losses resulting from loss of cargo
- Increasing insurance premiums
- Claims from frustrated staff members
- Brand and reputational damage
- Frustrated customers or suppliers

Risk Analysis

TAPA have developed a set of security standards to ensure secure transportation and storage of high-value, theft targeted cargo:

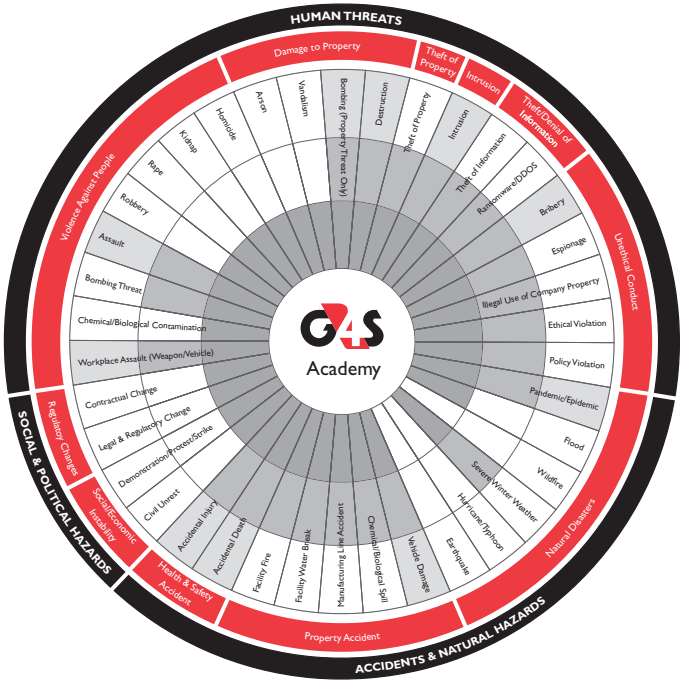
- The Facility Security Requirements (FSR) represents minimum standards specifically for secure warehousing, or in-transit storage, within a supply chain
- The Trucking Security Requirements (TSR) focuses exclusively on transport by truck and represents minimum standards specifically for transporting products via road within a supply chain.

TAPA global security standards are reviewed and revised as needed every 3 years.

We are often involved right at the start to evaluate an existing process and identify weaknesses and opportunities for improvement., assessing against the TAPA standards.

Our skilled teams of supply chain risk assessors can provide a detailed risk assessment from manufacturer right through to carrier, provide security audits and penetration tests and provide detailed reports on their findings.

These reports contain a clear security GAP analysis, against the published standards, supported by clear areas for corrective action.



Secure Technology

We supply a whole suite of systems to support your supply chain. The list below details each of the systems with a brief explanation of the functionality that they offer.

Component	Description
Telematics Device	GMS / GPS device providing real time position of the track and trailer. Available options: Capability to recognize jamming attack, Driving Behaviour analysis
Fixed Panic Button	Wired button installed permanently in the drivers cabin or next to the trailer's door connected to the telematics device input
Wireless Panic Button	RF button of short range connected to the telematics device input
Driver Authentication	Reader and tag (i.e. i-button) to recognize / authenticate the driver. Could be installed in combination with immobilizer to prevent ignition on by unauthorized drivers
Magnetic contact	Simple magnetic contact connected to the telematics device input to identify when the trailer door is open / closed. Advanced option available: security paired magnetic contacts that cannot be manipulated by a magnet.
2way communication Hands free	Can be used during distress by having silent listening in calls to evaluate the driver's condition.
Personal telematics device	GMS / GPS device providing real time position of the driver. Includes a panic button and could also allow man down events
Mechanical Trailer Lock	Heavy duty lock to prevent unauthorized access to the trailer
Electromechanical Trailer Lock	Permanently installed lock that is connected to the telematics device and can report the status of the lock (locked/ unlocked) but also can be controlled remotely.
Wire-net	Installation of a wire on the sides and the roof of the trailer, connected to the telematics device input to trigger an event when an attempt to cut an area of a hard sided trailer to access the cargo area
ADAS	Accident prevention system connected to the telematics device
G4S Mobility	Tracking platform decoding all telematics messages

Services

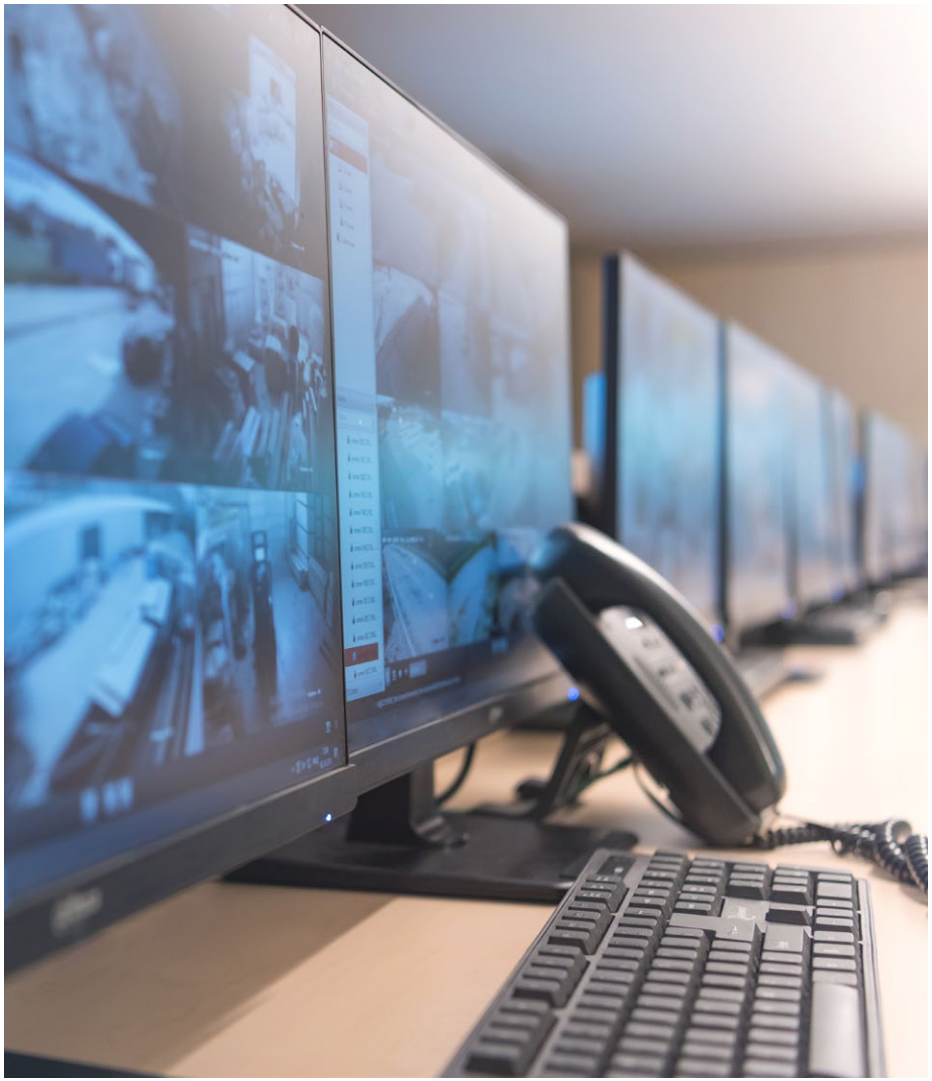
Underpinning the offering is our Security Control Tower which connects our systems, provides an initial response and triage and coordinates a physical response from our international network of Security Risk Operations Centers (SROCs).

This Security Control Tower is is one of the four Alarm Monitoring and Intervention Centers (AMIC) in Europe, approved by the leading manufacturers of High-Value goods and operates in compliance with EN50518.

The Security Control Tower provides active monitoring and immediate incident verification and validation, and dispatches the incident to the appropriate SROC which will follow an established incident management process which coordinates a response in alignment with pre agreed procedures.

The Security Control Tower establishes immediate two way communication with your device or staff member and then follows pre agreed protocols to deliver an appropriate physical response using our extensive European SROC network. These physical services may include (but not exclusively be made up of):-

- Police / Ambulance / Other Authority / Designated contact persons / Liaison
- Mobile Unit Dispatch and Onsite Response
- Dispatch of Static Guard onsite
- Cargo Escort Services



Quality in the Supply Chain

We are active members of TAPA and adhere to all principle standards. In the EMEA region, TAPA offers three industry standards:

- FSR – Facility Security Requirements
- TSR – Trucking Security Requirements
- PSR – Parking Security Requirements

TAPA's standards' programme offers three levels of certification by the Association's approved Independent Audit Bodies as well as a self-certification option.

TAPA's security standards act as a worldwide benchmark for supply chain security and resilience, providing guidance, processes and tools which reduce loss exposure, protect assets, help to keep staff safe and save costs.

Users of the standards are certified by a number of independent Audit Bodies which ensures certifications are meaningful and can be trusted.

Support for organisations using the TAPA standards comes from within the supply chain industry, by Government agencies and the insurance industry.

TAPA
Transported Asset Protection Association

The Security Control Tower

Our Security Control Tower is highly regulated and operates in resilient fashion on a 24*7 basis. We ensure that we will respond to all urgent cases in just minutes (in accordance with contractual SLA) and we'll monitor the case until it is resolved, keeping your staff and assets out of harm's way.

Our teams will communicate clearly with you, the progress of any incident and provide a full closure report when the incident is concluded.

An International Response Network

We offer a comprehensive European coverage through our direct network and network of partners with whom we coordinate a physical response when necessary.

Our Network.

G4S		THIRD PARTY		
Austria	Luxembourg	Albania	Georgia	Portugal
Belgium	Malta	Belarus	Germany	Romania
Czech Republic	Montenegro	Bosnia & Herzegovina	Hungary	Russia
Denmark	Netherlands	Bulgaria	Italy	Spain
Estonia	Serbia	Croatia	Kosovo	Sweden
Greece	Slovenia	Cyprus	North Macedonia	Switzerland
Ireland	Slovakia	Finland	Norway	
Latvia	Turkey	France	Poland	
Lithuania	Ukraine			
United Kingdom				

POSTSCRIPT

This whitepaper was written and produced by the G4S Academy and G4S Telematix teams.

This whitepaper may contain forward-looking statements including statements regarding our intent, belief or current expectations with respect to supply chain businesses and operations.

Readers are cautioned not to place undue reliance on these forward-looking statements.

The intention of this whitepaper is not to present a complete and all-encompassing view on security around cross-border transportation, but to elaborate and provide qualitative insights from G4S experts as a thought-starter for the creation of the supply chain security future of your organisation.

The information provided by G4S in this guide is for general informational purposes only.

We make no representation or warranty of any kind, express or implied, regarding the accuracy, adequacy, validity, reliability, availability or completeness of any information. Under no circumstance shall we have any liability to you for any loss or damage of any kind incurred as a result of the use of or reliance on any information provided in this presentation.

This guide and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales. The courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this document or its subject matter or formation.

BEYOND TRADITIONAL SECURITY

We'll go far beyond simple security delivery.

Our G4S Academy is open to all those that operate in the security industry and provides a unique opportunity for networking, CPD and a constant stream of intelligence - such as our weekly threat intelligence report.

Our G4S Academy providing a monthly security bulletin on potential as well as a repository of white papers, webinars and other continuous professional development material

Our Events and Seminars where guest speakers debate the latest market evolution and trends

Our Innovation Forum where we work closely with our customers to discus new security issues and how best to address emerging trends and technologies

Our Podcasts where we support continuous professional development through engaging debate - available at your leisure

G4S Academy

Listen to Noah's introduction and subscribe with our G4S Academy at
https://www.g4s.com/en-gb/what-we-do/academy

Contact Us

UK: 08459 000 447

enquiries@uk.g4s.com

2nd Floor, Chancery House,
St. Nicholas Way,
Sutton,
Surrey,
England, SM1 1JB

Ireland: 1890 447 447

g4ssales@ie.g4s.com