European Commission

EC Security Guidance for **the European Commercial Road Freight Transport Sector**

Mobility and Transport

The 'Publications Office of the European Union' has also published this toolkit in English language only:
ISBN: 978-92-79-77768-4 / doi: 10.2832/97074

TABLE OF CONTENT

OVERVIEW

The road freight transport sector faces many security threats today. Cargo theft continues to be a multi-billion-euro problem for the European transport sector. Irregular immigrants and terrorists pose additional security risks to international trucking operations – the former are boarding trucks clandestinely to cross borders, while the latter have turned heavy vehicles into weapons by hijacking and driving them into crowds.

To address these risks, Directorate-General for Mobility and Transport of the European Commission, DG MOVE, commissioned Cross-border Research Association (CBRA) of Switzerland and TAPA (as a subcontractor) to develop a new security toolkit for the European Road Freight Transport Sector.

This document is an abridged version of the ROADSEC toolkit. It aims at providing operational guidance that will help European truck drivers, haulage companies and other key stakeholders to address the above problems.

1/ INTRODUCTION

1.1. PURPOSE AND SCOPE OF THE WORK

This ROADSEC toolkit provides operational guidance that will help European truck drivers, haulage companies and other key stakeholders to address cargo theft, stowaway entry to trucks, and terrorism on European roads.

1.2. SECURITY RISKS IN THE TRUCKING SECTOR

Security risks in the context of (i) cargo theft, (ii) stowaway entry into trucks and (iii) trucks being used for terrorist purposes are briefly summarised and characterised in the three tables below.[1]

1.2.1. Cargo theft

Item	Cargo theft
Overview	Cargo theft is a worldwide problem. The complexity arises due to the different operating modes and types of cargo crime. The loss of value, cost of prevention, operating modes and preferred locations and preferred products vary across countries and regions. The losses incurred to the European Union due to cargo thefts are estimated to be 8.2 EUR billion annually, an average value of 6.7 EUR per trip.
Operating modes	A broad variety of operating modes can be regularly observed in the context of cargo theft, including: theft from a standing vehicle; robbery; hijack; theft from a moving vehicle; and, theft of vehicle and cargo. These acts of stealing property are often facilitated by "supporting measures", such as: fake identities, fake companies and fake police; document forgery; cybercrime; and even blackmailing and kidnapping (see the last table in this sub-section for more details).
Violence against drivers	In order to bypass different security features, a common method is to use or threaten to use violence against truck drivers (and/or terminal workers). The use of violence appears to lead to greater value goods being stolen. According to IRU, 17 % of all drivers suffered an attack during the past five years and 30 % of the victims were attacked more than once. 21 % reported they were physically assaulted during the attack.
Costs / negative impacts	The total cost of cargo theft incidents can be a surprise for logistics managers and law enforcement agencies, among other key stakeholders. Next to the (more obvious) costs for replacement of products (with product, logistics and administrative costs), one should also include at least the following cost categories: Security and investigation costs (proactive and reactive measures and actions); Insurance cost; and Costs for society (police, justice system etc.). For the (sectoral) quantification of such costs, further research is required.

1 Annex G of this toolkit contains a glossary with detailed definitions for (i) incident categories, (ii) criminal operating modes, and (iii) crime location types.

Eurowatch[2] has developed a threat/ risk matrix based on the road transport theft data over a seven-year period (2002-2009[3]), mapping operating modes and location of attacks against each other. Without a surprise, the various operating modes apply differently depending on the attack locations - the latter being described as transport stages from the consignor (load point) to the consignee (unload point).

ATTACK LOCATION / OPERATION MODE	Hijack	Robbery	Theft from vehicle	Theft of vehicle	Fake police	Fake accident	Deception
Load point	2	3	2	3	1	1	4
Driving	4	1	1	1	4	4	2
Unsecure parking	2	4	4	4	3	1	2
Secure parking	2	2	3	3	1	1	2
Near end location	4	3	3	4	3	1	3
Unload point	2	3	2	3	1	1	4

Low Risk **High Risk**

Figure 1.2 Cargo theft threat/ risk matrix (1 = lowest risk, 4 = highest risk)

The loading and unloading points are most risky for deception, meaning that a truck driver with a fake identity picks up a load from the consignor (and disappears with it), or a warehouse worker with a fake identity directs the truck to a fraudulent unloading point (and ultimately steals the cargo). While driving, the driver needs to be particularly aware of the risks of hijacking, fake police and fake accidents. Parking at an unsecure location makes the driver and load vulnerable for robbery, theft from vehicle and theft of vehicle; these risks clearly lower at a secure location. In addition, when approaching the delivery location, the risk of hijacking increases again.

2 A provider of cargo tracking and theft monitoring related services across Europe.
3 Although the data used to construct the matrix is from the last decade, the authors of this ROADSEC toolkit believe that the way it reflects the reality is (still) fairly accurate.

1.2.2. Stowaway entry into trucks

Item	Stowaway entry into trucks
Overview	Clandestine traveling or stowing away on board a truck is, in essence, a self-smuggling operation, where the perpetrator tries to smuggle himself into areas where he does not have legal access. The operating modes, the cost and losses of this activity might vary from country to country, but in general, this kind of activity puts in danger the life of the perpetrator, financially affects the driver and the road freight transport company and increases social and governmental costs.
Operating modes	Commonly, the perpetrator tries to sneak on board the truck when they are sure that the truck is heading in the direction they want to go and/or intending to cross a national border. While in the majority of cases this will happen close to the border crossing, there have been increasing numbers of incidents much further away from the border where there is a lower likelihood of detection. After the border crossing, the stowaway will aim to escape without leaving any tracks. In some cases, they may also steal goods from the truck or they may remove goods and leave them out of sight when boarding the truck in order to make space to hide.
Violence against drivers	Although violence against drivers is not very common, due to the obvious reason that the perpetrators desire to hop-on and hop-off the vehicle without being noticed, some violent threats towards drivers have been recorded which have involved the use of knives and other heavy implements used as weapons. The use of makeshift barriers on roads leading into ports, or the throwing of obstacles in front of a truck to make it slow down has occurred and resulted in numerous injuries and damage.
Costs / negative impacts	Several costs and negative impacts are associated with stowaways entering trucks. For drivers and the road freight transport company, they might face financial penalties even if they were not involved in the illegal act[4] and in some cases, cargo can also be stolen or damaged, or, it has to be destroyed if there is a risk of contamination. The life of the perpetrator might be in danger because the hiding place may not suitable for human transportation. Finally, as stowaways link to the broader irregular immigration problematic in Europe, the societal costs for policing, processing through the judicial system, social care, security infrastructure enhancements etc. play a significant role.

4 According to the UK Home Office, there are fines up to 2.000 GBP for the truck driver, levied for each stowaway found in the truck at the UK border.

1.2.3. Trucks being used for terrorist purposes

Item	Trucks being used for terrorist purposes
Overview	"Terrorism in all its forms, by its very nature, is an asymmetrical response to superior force, and terrorists have always used their capabilities as force multipliers – usually through the exploitation of terror. The generation of fear, in effect the use of purposeful violence as a form of psychological warfare can now be carried much further, enhanced by the modern media and the proliferation of mass media as much as by the proliferation of weapons". Within this context, there has been an unfortunate trend during the past couple of years of terrorist attackers weaponising trucks and vans by driving them through crowds of people in unprotected public areas of various European cities, including in Nice, Berlin, Stockholm, London and Barcelona.
Operating modes	The baseline MO is to drive a truck or van into crowded places to kill and injure as many people as possible. Some of these past incidents have also been combined with the perpetrator(s) leaving the vehicle to attack nearby pedestrians with knives. There have been some differences in how the truck was obtained, the timeframe for the attack and the attack location setup – additional details of five recent attacks in Europe (during 2016 and 2017) are described below.
Violence against drivers	Although serious violence, leading to death, was used by a terrorist against the truck driver in one of the five recent European incidents (in Berlin 2016), it is not possible to neither draw general conclusions nor provide predictions about the use of violence against drivers during possible future incidents.
Costs / negative impacts	Estimating and articulating the negative impacts of this category of terrorism is complex and affects many aspects of society. First, there can be an immediate cost to the driver, in case of injury, loss of life or at least livelihood if the truck is damaged/ destroyed. Second, there may be a cost to the operator – lost business, or reputational hit, particularly if the vehicle has a clear livery which ends up being shown in news broadcasts/ media, with the impression that the operator was not secure. Third, terrorist attacks are costly for the governments in terms of law enforcement, investigation, judicial and related costs. Fourth, the negative impacts in terms of human suffering, loss of life, impact on family and friends and so forth, can be enormous.

Lastly, the essential details of five recent (2016-17) terrorist attacks in Europe, where trucks or vans were exploited as terrorist weapons can be summarised as follows. To obtain the vehicles, renting (three incidents), stealing (one incident) and hijacking (one incident) have all been exploited by the attackers. The timeframe between obtaining the vehicle to the actual attack has varied from a few days (in Nice) to a few seconds (in Stockholm). Streets and market places with lots of pedestrians have been the targets in all five incidents.

1.2.4. Supporting / facilitating illicit operating modes

The last table below lists typical supporting / facilitating illicit activities that the target audience of this toolkit should be aware of - particularly relevant in the context of cargo theft (but also possible in the context of stowaways and terrorists). One should also be aware that interconnections often exist between various operating modes.[5]

Illicit MO	Explanation
False driver identities	A criminal can pose as a legitimate truck driver using false or stolen driver identities to steal cargo directly from a shipper/ warehouses. Other variations include the appearance of a recently terminated/ fired driver arriving in advance of his former employer's assigned driver.
Fraudulent companies	Using false or bogus carrier names, criminals pose as legitimate companies to trick other companies into handing their cargo over to them (commonly known as 'Fictitious Pick-up'). Because of the proliferation of internet access, it is relatively easy for criminals to set up online phony companies to win transportation bids and to obtain truck freight insurance. Various tricks include using websites to win transportation bids, or simply show up as drivers with fake credentials, claiming to be assigned to a load.
Fake delivery addresses	This MO occurs when legitimate drivers/ companies are deceived into delivering to a different destination than to the intended one (commonly referred to as 'Round the Corner'). This MO includes 'e-crime' where bogus logistics companies are established to divert the delivery.
Fake warehouse workers	Criminals can pose as legitimate warehouse workers and access warehouse systems to illegally approve the exit of goods or to divert the goods to a phony address. Alternatively, they can stand at a street corner close to the actual delivery location, aiming to divert the goods to a wrong address ('Round the Corner').
Fake police officers	Police impersonation is an act of falsely portraying oneself as a member of the police, for the purpose of deception. In the vast majority of countries, the practice is illegal and carries a custodial sentence. In some cases, criminals pose as fake police officers to force the driver to stop or to follow them to a specific location in order to steal the cargo.
Document forgery	Falsified versions of commercial or transport documents come in many different forms. They can be used to fake the sale of cargoes that do not exist, to illegally claim on Letters of Credit and waybills, fake Letters of Indemnity, as well as theft of cargo and / or cheating over quantity and quality.

5 Illustrative case from the United States, linking various facilitating illegal acts to cargo theft: "Thieves assume the identity of a trucking company, often by reactivating a dormant Department of Transportation carrier number from a government website for as little as 300 USD. That lets them pretend to be a long-established firm with a seemingly good safety record. The fraud often includes paperwork such as insurance policies, fake driver licenses and other documents. Then the perpetrator will offer low bids to freight brokers who handle shipping for numerous companies. When the truckers show up at a company, everything seems legitimate. But once driven away, the goods are never seen again".

Illicit MO	Explanation
Cybercrime	This MO involves data theft to identify loads, schedules, routes of the cargo. With this information, the criminals will intercept the goods before the legitimate owner arrives. Criminals can also alter data and therefore deceive the carrier, broker or client. For example, criminals can change the address and re-route the goods that will lead the cargo to fall into the wrong hands. In addition, the perpetrators can intercept and monitor communications to and from different actors in the supply chain to exploit information and perpetrate a whole range of frauds and other crimes from cargo related matters to smuggling activities. Lastly, cybercrime includes information phishing where fake emails are sent to different actors in the legitimate supply chain in order to obtain privileged information.
Blackmailing	Blackmailing can happen in different scenarios. Perpetrators target the driver or other personnel with a view to obtaining leverage over them and using that employee's fear of being exposed, in order to use their inside operational knowledge to access to the secure areas/ goods/ systems.
Kidnapping	This is a violent MO towards key personnel or relatives of key personnel to gain access to the right areas/ goods/ systems/ information.

1.3. ORGANISATION OF THE TOOLKIT

The main content of the ROADSEC toolkit is structured into the following chapters:

1. Introduction
2. Security guidance for truck drivers
3. Security guidance for logistics managers and key stakeholders

They are followed by the following annexes:

a. Top security tips for truck drivers
b. Security plan template: this is offered to managers responsible for producing and updating their company security plans, particularly in the logistics sector
c. Truck security checklist
d. Freight transport technology solutions: this annex introduces a template with some practical examples for storing and sharing basic information on solutions available in the markets for trucking security
e. Existing freight transport security standards: a brief introduction is made to the EU AEO (Authorised Economic Operator) Scheme, WCO SAFE Framework of Standards, UK Border Force and TAPA standards
f. Secure parking resources – a brief introduction is made to TRANSPARK, ESPORG, TAPA and European Commission initiatives
g. Security incident reporting forms: a brief introduction is made to CEN (European Committee for Standardisation) and TAPA reporting forms
h. Additional resources: brief references are made to EC DG MOVE on road transport policies, ADR regulations (on the carriage of dangerous goods by road), 'lone worker' regulations, and the European Agenda on Migration and Irregular Migration

2/ SECURITY GUIDANCE FOR TRUCK DRIVERS

As a driver, you are a potential target for criminals who want to steal your cargo; stowaways who want to cross borders hiding in your truck; and possibly terrorists who may want to exploit your vehicle and/or load for acts of terror. This guidance serves to protect you, your truck and your cargo. You are encouraged to adhere to these good security practices as part of your routine from picking-up your shipment to when you finally deliver it.

The first paragraph on general security applies across all journey phases, and Paragraphs 2.2-2.10 contain specific advice per journey and during each specific phase.

Visualisation of the Structure of Chapter 2:
General Security
Preparation
Pick-up
Driving
Stopovers
Control zones
Forced stops
Change in journey plan
Crime suspicion or incident
Delivery

Figure 2: Visualisation of the structure of Chapter 2

2.1. GENERAL SECURITY

The first paragraph of this Chapter highlights 22 key tips to minimise the risk of security incidents with thieves, stowaways or terrorists, in the freight transport sector. By systematically following this advice, you should be able to reduce potential security problems substantially, while undertaking your journey:

Guidelines	Clarification
Secure your vehicle and cargo, according to the company security policies and instructions.	• Be fully aware and familiar with your company security and customer level (shipment) obligations to secure your truck and cargo. • Be fully competent on all security features and devices within your truck including: - the panic alarm, - vehicle immobiliser, - telematics, - locks and seals; and - tracking devices.
Conduct visual checks around the truck, before departure and upon arrival.	• Always make sure that your vehicle is physically fit for purpose prior to commencing any journey, by conducting a visual check of the tractor and the trailer, verifying that the cargo contained within is secured and that there are no obvious mechanical anomalies. • Check for evidence of damage, tampering or unauthorised access attempts after every stop to verify that the load is safe from theft or stowaways.
Avoid high-risk routes ahead of every journey.	• Check intelligence warnings with police; check recent TAPA and insurance company incident reports etc. • Avoid known hotspots for cargo theft and stowaways.
Never carry goods for anyone else, other than the authorised load.	• In case someone asks you to carry additional items in the load, check with the back office whether you are authorised to do so.
Communicate revised journey plans or changing situations with the back office.	• Never change the route of your planned journey unless absolutely necessary. • In case you are required to revise your planned route due to unforeseen circumstances, including force majeure, always inform your back office in a proactive manner.
Do not change your delivery address without approval from the back office.	• The delivery address of your shipment is provided to you by your company / back office at the commencement of the journey. • Under no circumstances should your delivery address be changed during transit unless this is directly communicated to you by your company / back office.

Guidelines	Clarification
Do not communicate route or load details publicly, across social media or to persons unknown to you.	• Do not communicate or announce any aspect of your client, route, cargo, or destination across social media, radio or in any public place. • Criminals and thieves may be monitoring social media and radio communications in order to opportunistically target the loads.
Use only pre-approved, well-lit parking lots.	• As a minimum, use only well-lit and well-established parking areas, which are often highly frequented motorway service stations used by other truck drivers along main routes.
Keep your mobile phone fully charged, with important phone numbers stored in it.	• Always know in advance the phone numbers of who to contact in the case of a security incident or emergency along your route. • Make sure you know how to contact and coordinate with local police if a crime occurs.
Keep doors locked and windows closed.	• Ensure you keep doors locked and windows closed at all times while driving or stopped so that thieves, stowaways or terrorists will not have an easy entry into your cabin to compromise your safety and security – whether you are driving or while stopped.
Keep your truck keys secure and always with you.	• Take care to secure your truck keys at all times; never leave them unattended or for them to be easily identified and associated with your truck.
Keep your ID cards and wallet secure and out of sight.	• Ensure that your ID and wallet are safe and secure at all times so that thieves and stowaways cannot steal your ID and/or money, thereby compromising your journey and shipment.
Do not leave freight documents visible in your truck / cabin.	• Ensure that your freight documents are safe and secure so that thieves cannot identify the contents of your load.
Be aware that thieves might be breaking into your truck while moving.	• Be mindful of any slow-moving vehicles positioning themselves in front of your truck to cause you to reduce your speed. • Cargo thieves are also known to break into trucks and steal cargo even when driving full speed on a motorway.

Guidelines	Clarification

Be aware of the risk of attempts to deceive you (such as bogus police and staged accidents, and the risk of fake documents and bogus warehouse workers).	• Always be alert to the risk of bogus police or staged accidents
	  - Verify the bona fide of the police by requesting their ID while still in the cabin.
	  - In the case of an obvious staged accident, drive to the closest secure parking location, notify your back office and police authorities to validate the situation.
	• Your cargo may be at risk due to deception associated with fake documents and bogus warehouse workers who may deceive you to hand over your shipment at unmarked premises, typically near the delivery location.

Be wary of stopping, giving lifts to or accepting offers from anyone you do not know.	• Do not be targeted by unknown persons to you who may attempt to stop and befriend you as part of their ploy to rob you. • Do not stop or give lifts to anyone you do not know. • Similarly, do not accept drinks or food from unknown persons who may be surreptitiously trying to drug you to steal your cargo.
Stay vigilant at all times, as you are well placed to recognise potential illegal activities.	• Watch out for behaviours, events or any other signs that might indicate increased risk of theft, stowaways or terrorism.
Inform the authorities and the management of any security incidents immediately.	• All security issues and incidents related to the integrity of your vehicle and/or cargo should be immediately reported to the local police and to your back office.
Share experiences on security incidents with driver colleagues.	• Sharing can also include near-miss situations.
Attend security training sessions, when available.	• It can be useful to attend minimum one session per year. • The ROADSEC toolkit can be used as key content in the training sessions.
At all times, stay safe and secure, while avoiding being provoked into confrontations.	• Do not be antagonised or provoked into confrontational situations by thieves or stowaways as these situations may undermine your safety.
At all times, comply with local laws and regulations, including transport safety and personal safety.	• It is imperative that your personal safety and the integrity of your cargo are foremost in your mind during your journey. This can be achieved by complying with local laws and regulations.

2.2. PREPARATION

Being well prepared for each journey forms a cornerstone in effective and efficient freight transport security management, that goes without saying. You as a truck driver should follow this set of good security practices in order to mitigate the risk of cargo theft, unauthorised intrusion of stowaways or theft/hi-jacking of your vehicle possibly for use in a terrorist attack during the later phases of your journey:

Guidelines	Clarification
Obtain available security instructions from your back office, including any customer / load specific instructions.	• Prior to commencing your journey, ask your back-office planner or your manager if you are in doubt about any security instructions related to your load / shipment.
Plan your route before you start your journey, and decide where you are going to have stopovers and where to park overnight.	• Familiarise yourself with the entire route in order to minimise any security problems. • Online resources are available to support the planning.
It is important that the exact delivery time and location of your shipment is agreed with the end destination, before commencing your journey.	• In the event that you arrive early or are unable to meet the delivery deadline at the end destination, you should have an agreed alternative safe harbour location where you can wait for your delivery time slot.
Ensure that you adhere to your company or customer agreed No-Stop-Zones.	• In case of any deviations, communicate immediately with the back office to confirm.
Pre-book a lot at a secure parking place, if possible.	• Secure parking is a well-lit parking area, which as a minimum has a dedicated security barrier, perimeter fencing and CCTV coverage. • Be aware that the supply of prebookable secure parking lots is limited across Europe.
Avoid high-risk routes or routes where you need to drive slowly or make many stops.	• High-risk routes contain known hot spots where cargo crime regularly takes place or where stowaways are frequently active. • Stops and slow speed make you an easier target for any offenders.
Plan stopovers a considerable distance from high-risk border crossings or ports.	• There is an increased risk of stowaways entering your truck when you are close to border terminals. • When at a border crossing you should only stop where requested by authorities.
Make sure that all security related devices and features in your truck function properly.	• Typical security related devices include the panic alarm, vehicle immobiliser, telematics, locks and seals and tracking devices.
If a security check-list is mandated by your company, fill it in.	• A company specific security checklist can be built upon this ROADSEC security toolkit.

2.3. PICK-UP

The areas around the pickup location can often be an area of vulnerability. You should consider the following security recommendations at the pickup point to reduce the risk of interference with your cargo while it is in transit:

Guidelines	Clarification
Secure the cabin and remove the keys from the ignition.	• Consider turning off the engine during the loading.
Oversee loading to ensure that cargo is not missing or damaged and that there are no suspicious onlookers.	• Check that cargo matches transport documents (type, quantity and possibly weight). • Inform your back office about any deviations or irregularities. • Observe for suspicious onlookers watching the loading. • Ensure that no unauthorised individuals enter your vehicle. • Report any suspicious activity to the back office. • Note:"Oversee loading" does not apply when picking up preloaded semitrailers or when overseeing is not allowed by the shipper / customer.
Check that correct security seal numbers are written on the transportation documents.	• If written numbers are illegible on the documentation, contact the back office.
Check padlocks, seals, TIR cords and canvas for damage, right after loading.	• Physically check that padlocks are locked, seals are secure on doors, TIR cords are operational, and the canvas is undamaged.
Check that your navigation system finds the delivery address and make sure that you have the shippers and receivers phone numbers.	• Prior to departing the pick-up location ensure that the delivery address is fully confirmed.
Be particularly vigilant when leaving the pickup point as cargo thieves may try to follow you and target your load.	• Cargo thieves may try to attach a tracker on your truck as part of their efforts to track your journey. • If you believe you are being followed, keep driving, inform the back office, call the police, and try to get to a secure place.

2.4. DRIVING

While driving to your destination it is imperative that you remain alert to your surroundings at all times. Be aware that criminals are also capable of stealing your cargo while the truck is in motion – even at full speed - thus you should be aware of any suspicious activity around your truck:

Guidelines	Clarification
While driving, keep all doors locked, and windows closed.	• Cargo thieves, stowaways or terrorists may try to enter the vehicle, particularly when moving at slow speed, but also when moving at high speeds.
Keep a reasonable distance from vehicles in front of you so that you have the ability to manoeuvre the truck quickly if needed.	• Cargo thieves, stowaways or terrorists may try to force you to stop, for example by driving cars in front and behind your truck.
Watch out for vehicles that may be following your truck.	• If you suspect that you are being followed, stay calm and inform the police and the back office. • Do not speed or otherwise compromise traffic safety.
If you are accompanied by a team driver or a driver's assistant, ask him to monitor mirrors and camera systems to detect suspicious activities while you are driving.	• Pay attention to the mandatory rest periods, which may override this advice.
Do not pick-up passengers unknown to you.	• If you do pick-up unknown persons, there is a risk that these persons may be involved in cargo theft, stowaway smuggling or perhaps terrorism.

2.5. STOPOVERS

As cargo theft often takes place during driver breaks and overnight stops, it is important that you only stop at pre-approved, well-lit and secure parking areas. Please note that the risk of cargo theft as well as stowaway entry is high at public rest areas, laybys and parking lots, thus you should be guided by the following recommendations:

Guidelines	Clarification
Avoid stops close to origin and destination points of your journey.	• Cargo thieves are known to be active around industrial areas or cargo distribution centres. • In addition, refuel the truck and buy snacks or other supplies before the start of the journey, if possible.
You should stop only at secure locations, those which are preapproved, well lit or known to be secure.	• Online services such as Truck Parking Europe and TRANS-Park can guide you to find secure parking locations across Europe.

Guidelines	Clarification
If you have to leave your vehicle, park your truck where you are in a position to observe it.	• Plan to be in a position to observe your truck to ensure that no one attempts to interfere with it. • If possible, ask a person you can trust to watch your truck.
If you must stop outside a secure parking area, keep the break as short as possible.	• Inform the back office when and where you are stopping. • Avoid isolated, dark, or poorly lit areas with few other trucks.
If possible, park your truck with the loading doors against another vehicle, a wall or a building.	• This parking configuration makes it more difficult for thieves to access your cargo.
If you must stop when approaching a border crossing or ferry terminal, consider parking your truck facing the opposite direction or on the other side of the highway.	• Parking in this way may make potential stowaways think that you are driving away from the border they want to cross, not towards it, thus minimising the stowaway risk with your truck.
When you exit the cabin, close windows, lock doors, activate security devices, and always take the keys with you.	• Leave your truck unattended for the shortest time possible. • Activate trailer immobilisation device (if available) when you drop the trailer. • Check locks, seals, and security devices before and after every stop and report any evidence of tampering to the back office.
Before resuming your journey, look for any signs of damage, tampering or unauthorised entry.	• Check all security devices are intact and undamaged; if there is evidence of tampering or unauthorised entry immediately inform the back office and call the police. • When you enter your cabin, lock doors immediately behind you.
If resting or sleeping in your cabin, consider keeping the windows fully closed.	• Keeping windows fully closed makes it more difficult for thieves or terrorists to insert a tube with anaesthetic gasses.
Use common sense in cafes, restaurants and pubs – do not accept drinks from strangers or leave your drink unguarded.	• Be aware that thieves may attempt to target you and compromise you while you are stopped at a restaurant. • Unknown persons may surreptitiously try to interfere with your food and drink to drug you, so they can steal your cargo and/or vehicle.

2.6. CONTROL ZONES

Border crossings, seaports, and other controlled zones are security sensitive areas where special rules apply for vehicles and transported goods. When entering a controlled zone with your truck you should be aware that customs and other border control agencies may inspect your vehicle, cargo and/or transport documents. At the same time, you should be aware that criminals and stowaways may also operate in this area and you should therefore consider the following security advice when entering a control zone:

Guidelines	Clarification
In the event that you are required to wait for Customs clearance or other border formalities outside of the control zone, go to the nearest secure parking place and contact the back office.	• Having a predetermined safe harbour location in the vicinity of the control zone ensures that you can proceed quickly to a secure location, eliminating risk and uncertainty while you wait for your slot to cross the border.
If your trailer or container is resealed by Customs officers, document the new seal number and communicate it to your back office.	• Take a time stamped photo of the new security seal. • Ensure the integrity of the seal and that it has been properly affixed.

Please follow these special instructions at high-risk border crossings, for example before embarking on a ferry or rail shuttle to the UK and from North African harbours to Europe.

Guidelines	Clarification
Physically check the fabric, roof and security devices of the vehicle.	• If there is evidence of damage, tampering or unauthorised access, if possible take a time-stamped photo of the evidence and call the police and your back office. • Carefully check the panniers, wind deflectors and axles as stowaways may be concealed. • Check seal numbers and re-apply security devices.
Consider conducting a thorough manual check of the load and cargo space.	• This is particularly important if you were not able to secure your vehicle throughout the full journey.
Determine whether someone has tampered or gained access to your vehicle.	• Take a time-stamped photo of any evidence of tampering. • Report it immediately to competent authorities and your back office. • Do not investigate yourself or put yourself in any kind of danger.
If agreed with your management, record the checks made on your checklist.	• This could cover checks undertaken at loading, after every stop and before entering the control zone.

2.7. FORCED STOPS

A forced stop is defined as an impromptu stop along a route conducted by police or other competent authorities who are carrying out control and inspection activities. However, there is a risk that criminals can impersonate police officers, construct roadblocks and do whatever they can to deceive truck drivers to stop and to steal their load. You should be guided by the following recommendations so as not to be fooled by criminals to get you to stop:

Guidelines	Clarification
If stopped by police officers, only open the cabin window after officers have showed their badges.	• Immediately inform the back office and keep an open line of communications with the back office until police officers have proven their identity. • If you feel confident with officers' IDs, follow their instructions. • If you suspect that bogus officers are trying to stop you, call the police and your back office. • Always stay safe, and never resist.
If the police direct you to a police station, activate security devices and ensure that your truck and cargo are guarded while you are away from the cabin.	• Inform the back office that you are proceeding to the police station, giving them details of the location.
If you have any doubt concerning the authenticity of officers or any vehicle attempting to stop you, stay in your cabin with the engine running, and request to be escorted to the nearest police station.	• Stay in your cabin and keep your windows and doors locked. • Inform the back office that you have been stopped. • Do not do anything that would put you at risk.

2.8. CHANGE IN JOURNEY PLAN

From time-to-time, it may be necessary to change an original journey plan due to an unforeseen event along the route such as a traffic accident, major roadworks or flooding, among other possible causes. Any change to an original journey plan must be communicated immediately to the back office outlining the new route, revised schedule and stopover locations, as applicable. Consider the following recommendations to make sure that any change to the original plan does not expose you to unnecessary security risks:

Guidelines	Clarification
Avoid changing the journey plan which you have planned.	• If you must change your originally planned journey / route, inform the back office about the new route, revised schedule, stopover locations and any expected delays.
Query and confirm any requests to the change of delivery address.	• Be aware that cargo thieves may mislead you to deliver goods to a wrong address. • Call the back office to confirm the change.
If you get lost, keep calm and try to determine your location yourself.	• Call the back office. • Only then, ask passers-by to tell you your location (rather than directions). • Note that opportunistic cargo thieves may use your situation to guide you to an unsecure location.

2.9. CRIME SUSPICION OR INCIDENT

Despite taking all the necessary security precautions, criminals may still target the cargo in your truck. In the event that you witness a theft or suspect that thieves, stowaways or terrorists may be targeting you, it is recommended that you immediately call the police, inform your back office and follow these recommendations:

Guidelines	Clarification
If someone is stealing from your truck, do not leave the safety of the cabin. Lock the doors, start the engine, switch on the lights, and sound the horn to attract attention.	• Immediately call the police and inform the back office. • Push the in-vehicle panic button if you are in danger and there is a safe chance to do so.
If you believe you are being hijacked, try to keep your truck moving.	• Immediately call police and inform the back office. • Push the in-vehicle panic button if you are in danger and there is a safe chance to do so.
If confronted by thieves or stowaways, stay calm and avoid engaging with them, while not provoking confrontation.	• Stay in your cabin. • Inform police and back office. • Try to drive / escape to a safe location. • Resort to self-defence only if you cannot run away or if the offender threatens your or someone else's life. • Drivers should not subject themselves to the risk of criminal proceedings for mistreatment of stowaways or criminals.
Observe the situation, try to memorise as many details as possible and make notes on the incident situation as soon as you are safe.	• Support investigators as much as you can. • Your eyewitness testimony may help the police to investigate the crime and provide evidence for the prosecution.
Report crime incidents to the back office and the police as soon as possible.	• It should be noted that theft, crime or a security incident should be reported to the local police in the location where the incident took place (instead of at the final destination).
Ask the back office if you should contact your insurance company.	• Insurance experts may help you to reduce further damages and proceed with insurance claim.

2.10. DELIVERY

The area in the vicinity of your delivery destination can often be an area of risk and security vulnerability as criminals target your arrival. The following security guidelines are recommended prior to completing delivery of your shipment:

Guidelines	Clarification
Inform the consignee in advance about a change in the delivery time, either early or delayed, either directly or through the back office.	• The sooner the consignee knows about a changed delivery time, the quicker a revised unloading slot can be organised and the less time your truck is exposed to theft outside the consignee's premises.
Deliver only to the consignee and delivery address written in the transportation documents.	• Make no exceptions without approval from the back office.
Confirm that the consignee is the correct one and ask for identification.	• When making the delivery to a location or warehouse at a destination which does not show the name of the company, ensure that the load is handed over to the correctly identified consignee.
If available, follow a map and instructions received from the receiving company.	• When making a delivery, it is critical that a shipment is delivered to the correct location. If the delivery address location is not clear for you, obtain a map and instructions from the receiving company to ensure accurate reception.
Inspect seals for signs of tampering before the removal. Pull and twist standard band seals. Check that bolt seals spin freely in barrels and they have no glue on them.	• To ensure the integrity of the shipment at handover, validate with the receiving personnel that seals are intact and seal numbers are consistent with what is written on the consignment documents. • The driver should invite the consignee to inspect the integrity of the seals securing the shipment prior to removal.
Start facilitating unloading as soon as possible.	• Cargo is usually more secure inside premises, therefore avoid any undue delays to unload the goods.
Hand over transportation documents to authorised recipients only.	• Have proof of delivery signed by the consignee and send a copy of this proof electronically to the back office.
Monitor unloading operations personally if possible.	• On the completion of your journey, and if possible observe the unloading and delivery of the shipment from your truck at the warehouse.
If the delivery warehouse cannot take delivery on arrival, you should drive to the safe location which has been agreed in advance with the back office.	• You should have an agreed alternative safe harbour location in the vicinity of the end destination warehouse, where you can wait safely for your delivery time slot.

3/ SECURITY GUIDANCE FOR LOGISTICS MANAGERS AND KEY STAKEHOLDERS

3.1. INTRODUCTION

This chapter contains guidelines that logistics managers, other decision makers and key stakeholders may use to secure road transport operations from cargo theft, unauthorised boarding of stowaways, and terrorist hijacking. The guidance introduces a holistic risk assessment model, recommends good security practices, and summarises key principles for managing trucking security. This guidance is written mainly for managers who are concerned with trucking security, but some tips and advice are also applicable to security service and technology providers and the insurance sector as well as to police, border guard, and other law enforcement authorities. The management audience includes mainly:

- Fleet managers who organise trucking operations for trucking companies.
- Logistics planners who work for shippers and freight forwarders.
- Owner-operators who drive their own trucks.

Security needs for road transport vary from company to company. Factors like industry sector, type of business, nature of cargo and geography of operations determine which security risks are the most relevant for a company and which security solutions serve best the company's interests – "One size does not fit all" applies also in the context of trucking security. Trucking security management is essentially about matching security solutions to specific risks and needs, rather than implementing a predefined list of security measures. There are, however, certain commonly recognised steps, principles, and best practices that apply across most management situations. The paragraphs below introduce a five-step model that managers may follow to secure road transport operations from security risks.

Five-step model for managing trucking security risks:
Assess risks
Examine solutions
Compare alternatives
Implement decisions
Monitor results

3.2. ASSESS RISKS

The first step in security management is to recognise relevant security risks to trucking operations and to estimate related likelihoods and negative consequences. Risk assessment results reveal the nature and magnitude of security risks that shipments face during transport from origin to destination. This information helps managers to choose security solutions, which are commensurate to the level of risk.

3.2.1. Identify relevant security risks to your trucking operations

Various trucking operations are exposed to different security risks. For example, carriers of dangerous goods may face a high risk of terrorist hijacking, and foodstuff shippers can be vulnerable to hostile poisoning of their products. Managers should understand the special character of security risks that are relevant to their companies, as the managerial understanding of risks is crucial for the design of contextually sound security solutions.

Risk identification normally involves analysis of past security incidents, industry benchmarking, review of media and law enforcement reports, and collection of expert inputs. As the analysis of past incidents relies on quality data from previous security breaches, it is important to set up protocol for reporting security incidents. Preferably, the incident reporting should include detailed information: What happened? Where did the incident take place? When was it? Who was involved? How did it happen? To collect useful data to the latter question, incident reports could include the following characterisation of cargo theft operating modes.

Table 3.1 Operating modes of cargo theft

Operating modes	Description
Forced stop	Stationary barrier • Vehicle roadblock • Ramming by another vehicle • Drive-by shooting
Deceptive stop	Bogus police roadblock • Fake road works • Diversion from main route • Hitchhiker • Fake accident
Violence & intimidation	The use of force armed/unarmed • Threat to use force • Extortion
Deception	Posing as customer • Driver • Change of delivery details • Fraudulent delivery or release documentation
Intrusion	"Jump up" • Breaking door's lock or seal • Slashing tilt curtain
Insider crime	Active involvement in the theft by employee/s or driver/s

3.2.2. Estimate likelihoods & consequences of relevant risks

The next risk assessment step is to estimate likelihoods and consequences of relevant security risks to trucking operations. Past security incidents, industry benchmarking, and expert opinions usually help to estimate risk likelihoods, consequences, and overall risk levels.

Negative consequences of security risks are diverse. Economic damages are the most obvious consequence category of security incidents. Other consequences are reputational losses that, for example, shippers and carriers experience when they fail to deliver goods due to security problems. Compromised safety of truck drivers and the public is the third important consequence category of security risks in road transport. It is often difficult to quantify likelihoods and consequences, which often cannot be measured in terms of money or any other singular metric. Therefore, instead of calculations, managers commonly rely on qualitative (low – medium – high) expert judgements that consider various factors that drive trucking security risks. The table below presents some typical factors that affect magnitude of negative consequences of trucking security risks.

Table 3.2 Factors driving negative consequences of trucking security risks

Consequence	Factors driving negative consequences
Economic damages	Cargo thefts, stowaways on board or terrorist attacks may damage cargo, truck or other assets. Monetary losses include cost of goods sold, cost of replacing goods, cost of lost sales, contractual penalties, lost cross selling and upselling profits, and expedited remanufacturing and reshipping.
Reputational losses	For example, a late delivery of medical supplies may endanger patient safety, or a failure to deliver production critical components may harm a key customer relation. Product contaminations, due to terrorist tampering, may result in product recalls and ruin reputations overnight.
Work & public safety	Violent robberies and terrorist attacks may compromise work and public safety. Shipments of dangerous goods pose a higher risk if damaged, mishandled or stolen.

Likelihoods of security risks are also difficult to quantify due to the lack of reliable incident data as well as changing risk landscapes. As in the case of consequences, likelihoods are commonly estimated using qualitative metrics (low – medium – high). Managers should consider at least the following factors when estimating likelihoods of security risks for various shipments:

Table 3.3 Factors driving high likelihood of trucking security risks

Factor	Description
Routing	Transport through cargo crime hotspots increases the likelihood of theft. Traffic through border regions may increase the likelihood of stowaways boarding trucks. Driving near major public events may elevate the chance of a terrorist hijacking.
Transport schedule	Even though most cargo theft incidents take place during weekdays, loads should never be left in unsecured parking places or loading areas over weekends. Theft rates tend to be seasonal: slightly higher during autumn and winter than in spring and summer.
Distance and duration of transport	The more time a truck and its cargo spend on the road, the more time and opportunities criminals have to plan and commit crime.
Vulnerability of cargo	Theft-prone cargo is typically of high value, can be handled easily, and can be sold on the black markets for profit (see box below for characteristics of theftprone cargo). Dangerous goods may be vulnerable to terrorist hijacking. Foodstuffs, pharmaceuticals, and medical consumables are subject to a heightened risk of poisoning or other type of hostile product tampering.
Reliability of staff, middlemen, and subcontractors	The number and trustworthiness of people involved in road transportation operations determine the threat of insider collusion.

Characteristics and rating of theft-prone cargo

Certain cargo types are more attractive targets for thieves. Most theft-prone products are relatively easy to find, move around, hide, and resell later for profit. Here is an illustrative three-level scale that indicates how prone certain cargo types are to cargo theft:

Level 1 – Highest risk: Pharmaceuticals, especially those of high abuse potential; High-value electronics (e.g. cell phones and laptops); Cigarettes; Artwork, antiquities, and collectibles; Cash, precious metals, and precious stones.

Level 2 – Very high risk: High-end clothing; Cosmetics, perfumes, and personal care products; High-end foodstuffs (e.g. shrimp, lobster, and some meats); High-end metals, especially copper; General consumer electronics (televisions and computer peripherals); Over the counter drugs; Jewellery / Accessories.

Level 3 – High risk: General consumer goods; General foodstuffs; Building supplies and materials; Tyres and other auto parts.

3.2.3. Determine risk levels

The last stage of the risk assessment is to determine the overall security risk levels for shipments. The risk matrix is a common tool for comparing and visualising risks by magnitude and for evaluating whether a risk is acceptable or tolerable (or, cannot be taken). The higher the estimated likelihood and consequence of a risk is, the closer it gets to the top-right corner of the matrix. Less serious risks, that rank low on both likelihood and consequence, end up in bottom-left low-risk squares. The matrices below demonstrate the use of the risk matrix in a simplified shipment-level risk assessment. The haulage company used in the example transports mobile phones from East Europe to Central Europe.

CONSEQUENCES		Low	Medium	High
LIKELIHOOD	High		1	
	Medium			3
	Low		2	

	Risk	Likelihood		Consequence	
1	Cargo theft	Theft-prone cargo and route through theft hotspot	High	Contractual penalties	Med
2	Stowaways	Route through a typical stowaway route	Low	Fees and delays	Med
3	Terrorist hijack	Police warns about heightened risks	Med	Mass casualties and bad press	High

Figure 3.2: Example of risk matrices

The risk matrix shows that cargo theft and terrorist hijacking are the most important security risks for this specific shipment. This information allows managers to allocate limited security budget on solutions that lower security risks most cost-efficiently.

3.3. EXAMINE SOLUTIONS

The next step of the overall security risk management is to identify available security solutions that have the potential to lower security risks of trucking operations. The structure of this section is strongly inspired by the CBRA 8 layer model for supply chain security management (see figure below). Managers can follow these recommendations to shortlist solutions that best fit the needs of their companies and those of their clients. Because the first layer of the model on "risk management" has already been covered, the descriptions below focus on layers 2-8.

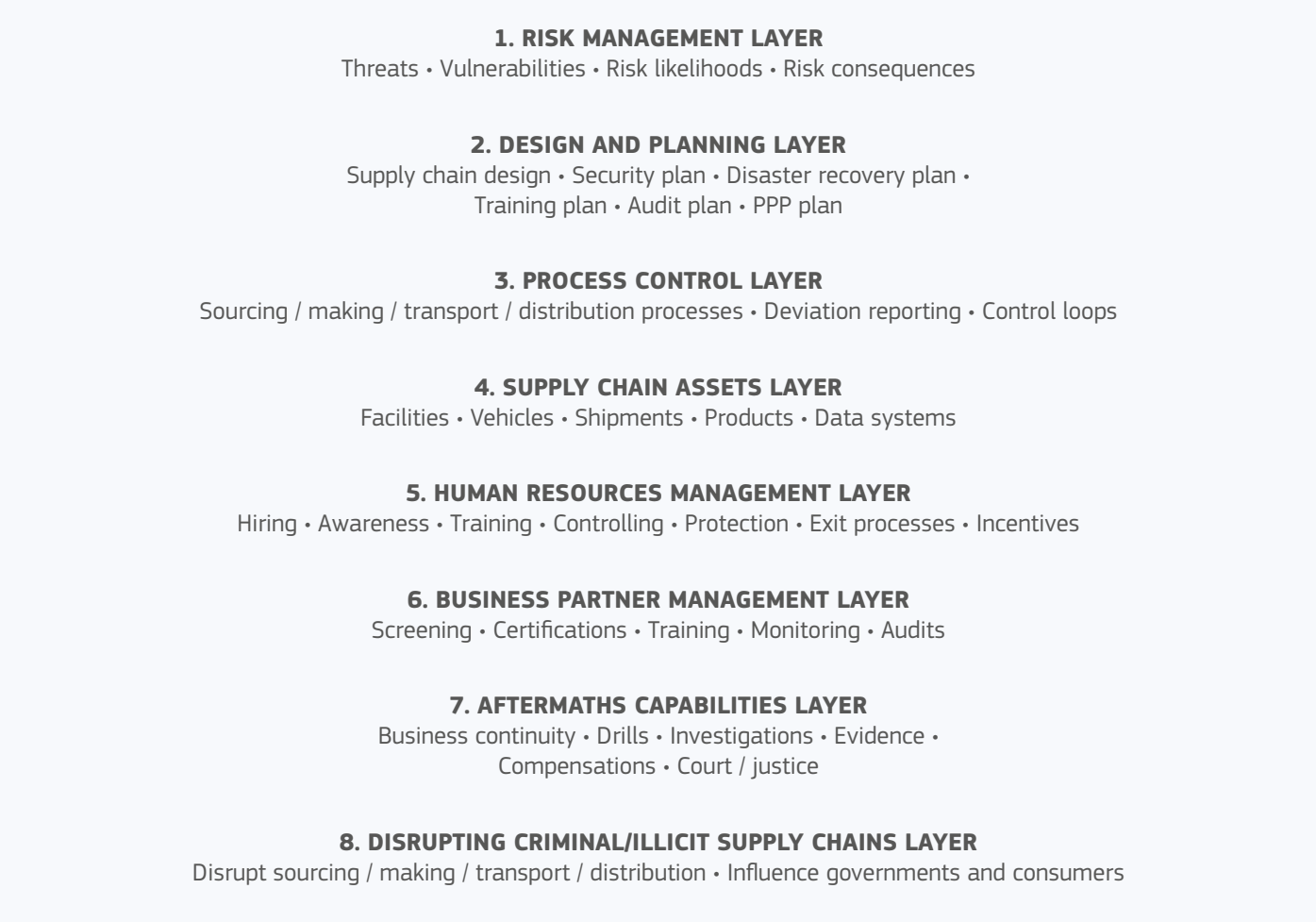

Figure 3.3 CBRA 8-layer model for supply chain security management

3.3.1. Design & planning

The design & planning layer covers proactive security management strategies that reduce exposure to trucking security risks. Follow these guidelines to design and plan security management:

Guidelines	Clarification
Route and schedule trucks so that drivers can always stop at secure parking locations (see box below on Parking place security).	• Use the IRU's TRANSpark application or a similar tool for locating secure parking lots. • Confirm opening hours and availability of free parking slots in advance. • A good practice is to plan each leg of the journey to last around 4 hours.
Alternate routes, stopover locations, and drivers.	• A recognisable pattern makes transport an easier target for criminals.
Introduce "no-stop-zones" and "no-drive-areas" where trucks must not stop or travel for security reasons.	• Obvious "no-stop-zones" and "no-drive-areas" would include known cargo theft hotspots.
Communicate pick-up / delivery details with the shipper / consignee prior to arrival.	• These details include the planned departure time, expected arrival time, driver name, the truck's license plate number, weight and piece-count of cargo, and trailer seal numbers (delivery only).
Consider shipping theft-prone cargo in smaller quantities to spread risk across multiple shipments.	• Consider also transporting components of theft-prone products in separate shipments. Assembly of high-end electronics could be done at the destination (postponement).
Consider major public events in scheduling and route planning.	• For example, major sporting events may slow down traffic and expose trucks to a heightened risk of terrorist hijacking.
Have a contingency plan in place to protect fleet and cargo in case of unexpected events.	• Possible contingencies include medical emergency, road accident, vehicle breakdown, unplanned detour, or the consignee's refusal to accept delivery.

Parking place security

The prevention of threats to the security of drivers and cargo is the fundamental reason to provide safe and secure parking areas. To this end, the European Commission commissioned a study on Safe and Secure Parking Places for Trucks, concluded in December 2018.

https://ec.europa.eu/transport/sites/transport/files/2019-study-on-safe-and-secure-parking-places-for-trucks.pdf

The study finds that current standards for safe and secure parking areas (e.g. LABEL, VEDA, PSR) vary greatly and that many of these areas are not audited, which causes uncertainty among users on the level of safety and security and on service levels provided to drivers. The study also finds that booking safe and secure parking spaces for drivers in advance is often not possible or at best unreliable and cumbersome.

In response, the study proposes a common standard for safe and secure parking areas – 'EU-Parking' - ranging from a low level (Bronze) to medium (Silver) to high (Gold and Platinum), all with the same minimum service levels for drivers in terms of sanitation, restauration and comfort. The study also proposes audit procedures, standard APIs (Application Program Interfaces) for booking systems as well as practical and financial guidelines for promoters on how to develop safe and secure parking areas.

3.3.2. Process control

The process control layer is about building visibility and control mechanisms for trucking operations so that any suspicious events – including strange route choices and unexplainable stops – can be detected and investigated as fast as possible. Follow these guidelines to control security of trucking operations:

Guidelines	Clarification
Stay abreast of the evolving security risk landscape.	• For example, TAPA publishes regular updates on cargo theft situation and hot spots.
Instruct drivers on how to cope with unexpected events.	• Drivers may get lost, need an unplanned break, or have to change route due to heavy traffic or other reasons.
Provide drivers a radio for two-way communications and/or a hands-free mobile phone with preprogrammed contact numbers.	• Important contacts include the consignee, the local police, and the 24/7 back office contact.
Fully use all media capabilities of smart phones to communicate with drivers.	• For example, send a picture of the consignee's premises to the driver to minimise the risk of delivery to a wrong address.
Monitor telematics data to detect deviations from original plans.	• Unusual routing, stopovers, or procedures may relate to security issues.
Consider setting up virtual technological barriers called geo-fences (see box below for details).	• Geo-fences are a good way to enforce that trucks do not enter "no-drive-areas".
Consider installing tracking devices on trucks and trailers.	• Prepare protocols for managing situations when tracking information raises suspicions, for example due to strange routing or unexplainable stops.

Guidelines	Clarification
Consider adding hidden tracking devices to theftprone cargo units.	• Trackers may help to recover stolen cargo and/or vehicles.
Monitor fleet management reports to detect idling vehicles.	• Trucks left unattended with the engine running are vulnerable to hijacking.
Oversee the behaviour of truck drivers.	• Monitor the tachograph information of truck drivers. • Encourage, for example, customers and other drivers to report suspicious behaviour of truck drivers.
Establish procedures for collecting security incident reports from drivers.	• Consider using standard reporting forms such as cargo theft incident reports of TAPA or CEN.

Use of geofencing in trucking security

Many trucking companies exploit track and trace solutions to keep tabs on their fleet and cargo. Asset-monitoring is used primarily to optimise haulage operations but also to strengthen trucking security. One way to use track and trace in security is geofencing, a practice of setting up virtual technological barriers around designated areas. With geofencing, managers can determine “no-drive-areas” where trucks are not allowed to enter and “secure transport corridors” from where trucks are not allowed to exit. When the geofences have been activated, the management receives a warning if a truck goes off-route by crossing a geofence. Managers should consider these recommendations to use geofencing effectively for security purposes:

- Set up and update geofences based on security intelligence. For instance, designate “no-drive-areas” to avoid cargo theft hotspots and “secure transport corridors” to navigate across high-risk regions.
- Mount trackers on tractors, trailers, and security-sensitive cargo units.
- Prepare a security protocol for managing geofencing warnings.
- Consider installing security devices that can be activated remotely when trucks enter “no-drive-areas” or exit “secure transport corridors”. In case of a geofence breach, for example, electronic locks would not open, trailer could not be dropped, or engine power would be reduced (to slow down potential hijackers).
- Purchase tracking devices that are robust to cyber-attacks, signal jammers (devices that prevent the trackers from receiving and sending messages), and spoofing attempts (a technique to manipulate geographical coordinates, that the trackers send, to make it appear as if a stolen truck was still on its planned route).
- Explain to truck drivers why geofencing is important.

3.3.3. Asset protection

Physical protection of cargo, trucks, trailers, and information systems is still the centrepiece of any trucking security system. Follow these security guidelines to increase physical and data security:

Guidelines	Clarification
Prioritise hard-sided trucks and trailers.	• If hard-sided vehicles are unavailable, use slash resistant curtains and sealed / padlock TIR cables to protect soft-sided trucks and trailers.
Pay special attention to security of loaded trailers.	• Loads should never be dropped awaiting unloading, or kept in yard storage over weekends or holidays.
Consider providing drivers with a panic alarm button.	• When installing the panic alarm button in truck cabins, ensure that drivers can push the button unnoticed.
Consider installing pin locks, landing gear locks, and brake-line locks and tractors with steering gear locks, airline locks, and audible burglar alarms.	• Security solutions should conform to appropriate standards.
Consider installing jamproof tracking units.	• Cargo thieves are known to user jamming devices to disable tracking devices.
Fit extra lock reinforcement at the rear on the cargo/container doors.	• Criminals can often break standard locks in seconds with basic tools.
Consider installing cargo space microphones, heartbeat detectors, and/or CO2 detectors.	• These technologies help to detect stowaways.
Lock access to the on-Board Diagnostic port.	• Thieves and terrorist may use the port to bypass locks and immobilisation devices and start the engine.
Alternate the type of security seals (colour and shape) and issue seal numbers in random order to make it more difficult for criminals to anticipate specific seal numbers	• Cargo thieves are known to use 3D printers to produce fakes. • Ensure that records for security seals are maintained and audited regularly.
Create and maintain a key holder record.	• Instruct drivers and other key holders to report immediately if their keys are lost or stolen.
Consider intelligent cargo placement when loading.	• If possible, instruct drivers to place high value cargo near the back of the cargo compartment and to surround the valuable cargo with less valuable cargo.
Consider introducing double drivers and security escorts to protect vulnerable shipments.	• Be aware that overt security escorts may signal to criminals that a load is worth stealing.

Guidelines	Clarification
Use tamper-resistant or tamper-evident packaging.	• Tamper-resistant and tamper-evident packaging is particularly important for food, pharmaceutical, and other sectors that are highly vulnerable to hostile product tampering.
Avoid logos or other branded features on trucks or packaging.	• Visible brand markings may attract thieves. • Place branded boxes inside plain boxes.
Protect computer systems and data from unauthorised access with strong passwords, antivirus software, firewalls, and other cyber security measures	• Criminals may break into information systems to obtain sensitive logistics information (e.g., loads, routes and schedules). • Weak cyber security helps criminals to circumvent electronic physical security systems, like vehicle immobilisation devices, trackers, and smart seals.
Consider consulting security professionals and reviewing security standards (see box below) before purchasing /installing / configuring physical security systems.	• Standards provide information on how to select appropriate security solutions for a given purpose.

Standards and trucking security

Various security standards provide useful information that managers should consider when they design trucking security and purchase security products and services. For example, the Transported Asset Protection Association (TAPA) maintains three certifiable key security standards, which trucking companies should be aware of:

- 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.
- The Parking Security Requirements (PSR) represents minimum standards specifically for secure parking places and used by vehicles intended for the movement of goods by road.

There are also many regional and national norms that provide technical performance criteria for a variety of trucking-relevant security solutions, including:

- ISO 15638:15-2014 Intelligent transport systems: vehicle location monitoring, form and content of data, high-level definition of the service that a service provider has to provide.
- EN 50518 - Monitoring and alarm receiving centre: security systems in buildings, functional performance criteria and verification of performance.
- ISO 18185-3:2015 Freight containers. Electronic seals. Environmental characteristics: locking and locating devices, environmental testing, crime prevention.
- ISO 17712:2013 Freight containers. Mechanical seals: the classification, acceptance, and withdrawal of mechanical freight container seals.
- EN 12320:2012 Building hardware. Padlocks and padlock fittings. Requirements and test methods.
- EN 50131-1:2006+A2:2017: Alarm systems, Intrusion and hold-up systems. System requirements.
- EN 62676-4:2015: Video surveillance systems for use in security applications. Application guidelines.

3.3.4. Human resource management

Vigilant employees who are willing and able to prevent and detect security breaches are crucial for effective trucking security. Consider these recommendations to develop security competence of truck drivers and to determine trustworthiness of other personnel:

Guidelines	Clarification
Appoint a person responsible for trucking security.	• This person should be competent in security matters and preferably a senior staff member.
Vet backgrounds of drivers before recruiting them (for example, criminal record and history of drug abuse if possible).	• Check details until you are comfortable. • Ensure consistency with national legislation.
Incorporate security duties and responsibilities into employment contracts.	• Emphasise the importance of security to new truck drivers. • Enforce that drivers follow security protocols.
Set incentives for drivers to comply with security procedures and to remain vigilant.	• For example, reward drivers for exemplary security work; discipline those who fail to carry out their security duties.
Build security awareness among drivers.	• For example, keep security posters in common workspaces, hold security workshops, and send email reminders. • Instruct cargo handlers / gatekeepers to remind truck drivers of security protocols.
Involve drivers in security planning and monitoring activities.	• Talk to drivers and encourage them to share their views and provide feedback.
Organise training for truck drivers and provide them with written instructions and checklists.	• Instruct drivers on how to manage seals, trailer door locks, pin locks, and other security equipment. • Explain to drivers the importance of following security protocols. • Refer to Chapter 2 and Annex A.
Limit the number of people who know the details of trucking operations.	• Information about clients and loads should be kept secure and shared on a need to know basis.
Trust high-value or highrisk loads only to experienced and trustworthy drivers.	• Consider using two drivers to transport sensitive loads.
Establish a security policy for the use of smart phones and devices as well as social media (see box below).	• Criminals may exploit information that truck drivers post on social media.
Create a plan for dealing with blackmailing or kidnapping of drivers.	• Consider purchasing an insurance against kidnapping, especially for drivers working in high-risk countries.
Discuss security issues with other managers, both inside and outside of your own company.	• Exchanging views and experiences with other managers is crucial to keep updated on trucking security.

Role of social media in trucking security
As many truck drivers are becoming increasingly active on social media, it is reasonable to instruct them about the secure use of Facebook, Twitter, Instagram, and other social media services. Criminals are known to scan social media to identify people and locations and to gather information about attractive targets. Careless use of social media exposes drivers to unnecessary risk of robbery, blackmailing, and other crimes. Consider these recommendations when you instruct drivers on how to use smart phones and devices as well as social media: • Do not post information about cargo, clients, route, or schedule on social media. • Do not share photos along your driving route, as the photos often include visual cues, timestamps, and geographical coordinates that give criminals hints about your whereabouts, your vehicle and the cargo on board. • Do not accept friend / follower requests from people you do not know or trust. • Turn off location sharing applications when driving (for example Foursquare). • Manage privacy settings (no public profiles). • Do not change your travel plan based on news or information published on social media, as fake information may lead you into danger. • Have strong passwords and keep them safe. • Consider enabling two-factor authentication and other advanced security features to protect your account from hacking.

3.3.5. Business partner & stakeholder management

Cooperation with business partners, authorities, and other key stakeholders is a cornerstone of effective trucking security. Consider these guidelines to maximise security benefits from cooperation:

Guidelines	Clarification
Create security criteria for selecting trucking companies, freight forwarders, and other logistics and transport service providers.	• Consider referring to the TAPA Trucking Security Requirements (TSR) or similar security standards.
Create a list of trucking companies that meet the security requirements of your company.	• A list of secure trucking companies facilitates logistics planning. • Consider cooperating with business partners to produce white lists of reliable logistics service providers. • Use only well-known / trustworthy carriers with your high-value or high-risk loads.
Verify backgrounds of trucking companies and buyers of goods.	• Check details until you are comfortable.
Monitor and audit security performance of the trucking companies.	• You can opt to follow the Security Performance Indicators (SPIs) as listed in Paragraph 3.6.1 of this document.
Build and foster security relationships with trucking companies, forwarders, and other logistics operators.	• Consider, for example, negotiating mutual parking agreements at secure parking places with other trucking companies.

Guidelines	Clarification
Involve business partners in security planning.	• Discussions with business partners may provide new useful perspectives on the trucking security of your company.
Liaise with local police and other competent authorities.	• Cooperation with the police increases chances of recovering stolen cargo.

Fraud on online freight exchange sites

Use of online freight exchanges, marketplaces for selling and buying transport capacity, has become commonplace in the road transport sector. Matching loads with capacity, the freight exchange services offer shippers cheaper prices and increased flexibility and carriers more efficient use of transport capacity. Both shippers and carriers use freight exchange services normally without any problems, thanks to advanced security controls of many providers, like TimoCom and Teleroute. Even so, unsuspecting shippers occasionally contract fraudulent carriers that pick-up cargo but never deliver it to the intended destination. Shippers may follow these recommendations to avoid falling victim to freight exchange fraud:

- Do not book transport for theft-prone goods on online freight exchange sites.
- Allow only trusted personnel to buy services on freight-exchange sites.
- Check if your load is re-listed on the freight-exchange (subcontracting).
- Crosscheck the carrier's e-mail and phone numbers with the company's official website.
- Check the carrier's address on Google street view.
- Follow up on the delivery with the consignee.
- Ask the carrier to send the following documents:
  - The company's licenses and permits, VAT number, proof insurance and client references.
  - The driver's full name, phone number, and copy of his license.
  - The vehicle's registration details and license plate number.
- Verify documentation and ask for clarification if in doubt.
- Be particularly vigilant if:
  - The carrier asks about the value of goods.
  - The driver changes unexpectedly.
  - The requested documents are incomplete or details differ from the information in the freight exchange platform.
  - The company does not have a professional website.
  - The ownership in the company has recently changed.
  - The carrier communicates via Skype, generic email addresses, or any other unconventional channels.

3.3.6. Aftermaths capabilities

Aftermaths capabilities seek to facilitate investigations of security breaches and ensure that past security incidents are considered in future logistics planning. Consider these good practices to improve capability to cope with the aftermath of trucking crime:

Guidelines	Clarification
Create contingency plans and supportive training materials.	• These plans help your company to deal with the aftermaths of security incidents and to identify weakness in aftermath capabilities.
Advise drivers how to behave in threatening situations.	• Remind the drivers to stay calm and avoid confrontation.
Establish communication and reporting procedures to collect driver feedback and help the drivers to report suspicions and crime incidents.	• Provide drivers with incident reporting forms and train them to complete them. • Consider setting up anonymous offline and online channels for providing feedback and concerns.
Consider serialising cargo units.	• Numbering may help to investigate theft incidents.
Trucks and trailers can have distinctive colours or markings (not descriptive text identifying the cargo being hauled) so they will be easy to identify if stolen or hijacked.	• Special markings on roofs of tractors and trailers help to identify them from above with drones or helicopters.
Cooperate with police investigators.	• Close cooperation with investigators may increase chances of recovering stolen cargo.

3.3.7. Disruption of criminal activities

One way to lower the risk of crime and terrorism is to disrupt activities of cargo thieves, stowaways, and terrorists. Consider these tips to make it costlier, risker, and less rewarding for them to commit crime and inflict damage on trucking operations.

Guidelines	Clarification
If trucks must access major public events, reduce the capability of a potential terrorist to accelerate a truck into a crowd by employing vehicle barriers.	• Coordinate the set-up of entry barriers with event organisers.
Monitor online markets to identify sellers of stolen goods.	• Making sales of stolen goods riskier lowers incentives for theft cargo.
Introduce product features that complicates the resale of stolen goods.	• Such security features include PIN-codes for electronics, for example.

3.4. COMPARE ALTERNATIVES

The next step, after managers have identified possible security solutions, is to compare alternatives and to decide which solutions to implement. The guidance of this section clarifies a set of preconditions, various cost categories, and different outcomes of security investments of which managers should be aware when deciding on trucking security solutions. This guidance helps managers to understand various trade-offs with potential security solutions and to make well-justified investment decisions.

3.4.1. Understand preconditions of security solutions

Most trucking companies face barriers and limitations that prevent implementation of certain security solutions. These preconditions vary from company to company, depending on factors like company size, range of operations, and organisational culture. Because not all security solutions are feasible for all trucking companies, managers should study which of the four main types of preconditions limit their decisions:

- **Availability** determines whether a security solution can be implemented at all. Some countries, for example, prohibit drivers' preemployment background checks on privacy grounds. Similarly, security-aware route planning and "no-stop-zone" policies must consider conditions of driving time regulations. Besides legal constraints, lacking infrastructure may limit availability of security technologies. For example, some geolocation technologies stop functioning in regions without mobile network coverage.

- **Level of expertise and guidance** restrict the implementation and use of many security solutions. Truck drivers must know, for example, how to deal with security seals, to switch on tracking devices, and to locate secure parking places. Expertise and proper instructions are also needed to install, configure and maintain security technologies. Installation of CCTV systems, for instance, requires understanding of effective location and orientation of cameras to maximise their benefit.

- **Practicability** refers to the convenience of use of a security solution. Truck drivers tend to disregard cumbersome security protocols. A driver might, for example, stop locking doors or using security seals if he needs to open trailer doors at multiple locations during his pick-up / delivery round. It is therefore crucial to design user-friendly and fit-for-purpose security solutions that match specific conditions and requirements.

- **End-user commitment** is the fourth main precondition of trucking security solutions. Truck drivers should be made aware of how security solutions benefit them, the trucking company, and wider society. Rewards for exemplary security work and other incentives can help to build strong driver commitment to security.

3.4.2. Estimate costs of security

Business realities and management priorities set budget constraints for security investments. Managers should, however, consider also procedural, ethical, and other non-monetary costs when they compare alternative security solutions. Here are the three main cost categories of trucking security:

- **Monetary cost.** Most security solutions involve a fixed one-time implementation cost and a recurring variable cost. Implementation costs cover spending on security equipment, installation, and initial training. Variable costs include costs of the actual use and maintenance. Managers should talk with subject matter experts, vendors of security solutions and company controllers to estimate accurate lifetime costs of various trucking security solutions.

- **Procedural cost.** Procedural costs are incurred when security solutions complicate or slow down trucking operations. For example, security-aware routing around high-risk crime areas / "hotspots" may incur costs in terms of delays or extra coordination requirements. Another example is a cumbersome locking and sealing procedure that consumes time whenever a driver needs to open trailer doors.
  Moreover, security entry protocols at depots, ports, and secure parking lots often take time and therefore may incur a procedural cost.

- **Ethical cost.** Ethical costs are incurred when security solutions discriminate against individuals or social groups, for instance, when a trucking company does not hire drivers from a certain social group for security reasons. One variety of ethical cost is distrust between company management and truck drivers, which stems from security solutions that drivers consider invasive or unfair. Routine background checks, 24/7 tracking systems, and bans on social media use are examples of such security solutions that may disturb drivers and undermine trust if the reasons for implementation are not properly explained.

The box below provides another perspective on costs of trucking security by elaborating concepts of mandatory security management, proactive security management, and reactive security management.

Cost considerations of trucking security management

Trucking security involves mandatory security management, proactive security management, and reactive security management. Cost of mandatory security management involves expenses that are incurred when a company complies with obligatory security laws and regulations. For example, carriers of dangerous goods must comply with provisions of the European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR). Because mandatory costs, at least in principle, are fixed and cannot be avoided, the real challenge of cost-efficient trucking security is to balance costs of proactive and reactive security management. The proactive security management is about investing in security that goes beyond the mandatory regulatory requirements, for example extra locks, 24/7 asset monitoring, and security guards. The reactive security management, in turn, involves costs of security incidents (e.g. value of stolen goods and cost of re-shipments) as well as lost security benefits (e.g., better on-time delivery performance and staff retention rates). Reactive costs tend to decrease when proactive costs increase because with more proactive security in place, typically fewer security incidents will occur. Mandatory costs remain the same regardless of the allocation between proactive and reactive costs. The total cost of trucking security management equals the costs of the three cost components: mandatory, proactive and reactive.

3.4.3. Assess expected outcomes

Security solutions are designed to lower the risk of crime, stowaways and terrorism to trucking operations. Outcomes of security solutions, however, are sometimes unexpected. Sometimes security solutions backfire and expose trucking operations to higher risk. On the other hand, in more opportune instances security solutions may boost operational performance or result in other unforeseen collateral benefits to the trucking company:

- **Reduction of security risk** is the main purpose of trucking security. As explained earlier, risk reduction can be achieved by lowering likelihood and / or consequence of any security risk. Managers should estimate risk reduction potential of alternative security solutions before deciding which solutions to implement.

- **Reverse effects** can occur when security solutions backfire and cause unintended negative effects. Criminals commonly change their behaviour in response to new security solutions: some stop committing crimes, but many just change targets, operating modes, locations, and/or timing. For example, if reinforced locks prevent breaking into trailers, some cargo thieves might start using violence to get the keys from truck drivers. Another possible victim of a reverse effect is a trucking company that starts using electronic shipping documents and this way exposes shipping information to cyber-attacks and sabotage.

- **Collateral benefits** - sometimes security investments can also improve business performance. For example, asset-monitoring solutions often not only increase security but also enable better operational planning and faster response to logistics contingencies. RFID-based identification of trucks and trailers may speed up entry into logistics depots, ports, and secure parking areas. Security may also lead to better customer satisfaction and higher brand protection because fewer shipments are delayed or lost due to security incidents.

3.4.4. Decide on security solutions

When managers decide on security solutions, they should consider preconditions, estimated costs, and possible outcomes of alternative security solutions. In addition, key business partners and staff members should be involved in the decision-making process. After thorough consideration, company managers should select the most promising and feasible solutions and plan their implementation.

3.5. IMPLEMENT DECISIONS

The implementation phase follows when company management has compared and ranked available security solutions and decided on which solutions to adopt. Effective implementation of trucking security solutions depends largely on proper planning and coordination. Managers should ensure availability of adequate resources – including money, time, skills, and expertise – and establish mechanisms for monitoring budget and schedule of the implementation.

3.5.1. Assign security roles & responsibilities

Committed and competent people are key to effective implementation of security solutions. Managers should assign security roles to staff members. Defined roles clarify responsibilities for deploying, using, and maintaining new security solutions, among other important tasks. Security responsibilities should be documented and communicated to relevant employees, contractors, and other stakeholders, highlighting the importance of security. Access to sensitive security information should be restricted to only trusted people who need it to carry out their jobs.

3.5.2. Train drivers & other personnel

New security devices often require training of drivers and other people whose responsibility it is to operate and maintain them. Produce and distribute training material like checklists, manuals, and videos among relevant staff and organise training workshops or on-the-job training as needed. Ensure that the training has desired impacts on skills and knowledge of drivers and other personnel.

3.5.3. Deploy solutions

Deployment of security solutions sometimes requires changes in original implementation plans. Be ready to revise implementation plans particularly according to feedback from drivers. The feedback might, for example, reveal that new security solutions are too easy to circumvent or that they overcomplicate drivers' work or invade their privacy, thus calling for revisions.

3.6. MONITOR & REVISE

Security threats are changing constantly, and implemented security solutions might not work as planned. To stay abreast of security challenges, managers should continuously monitor security performance and revise security plans for effectiveness and efficiency. Constant monitoring helps the managers to understand how security solutions perform: whether, to what extent, and under which circumstances security activities lower security risks. Performance monitoring also helps to organise day-to-day trucking security, redesign security activities, justify security investments, and to monitor the progress of ongoing security initiatives and efforts.

3.6.1. Establish & monitor security performance indicators (SPI)

Security performance indicators inform effective trucking security management: the classic management proverb "if you cannot measure it, you cannot manage it" holds true also in the trucking security context. The most suitable set of Security Performance Indicators (SPI) will differ from company-to-company. Below is a list of SPI examples that trucking companies and shippers may consider adopting. Company security policy should determine targets for each indicator and outline strategies for achieving them.

Table 3.4 Security Performance Indicators (SPI) for trucking security (List not exhaustive)

Category	Security performance indicator (SPI)	Unit	Data source
Completeness	Stopovers at security parking lots	[%]	Stopover record
	Shipments secured with solution X	[%]	Security solutions record
	Security trained drivers	[%]	Training log
Cost efficiency	Cost of security per shipment	[€]	Accounting
	Cost of security to sales revenue	[%]	Accounting
	Percentage of false alarms	[%]	Incident reporting
Effectiveness	Average security-related loss per shipment	[€]	Accounting / industry reports
	Total security-related losses to sales revenue	[%]	Accounting / industry reports
	Rate of security incidents (actual and attempts)	[%]	Incident reporting
	Security audit score	[n]	Audit reports
	Driver belief in security	[1-5]	Driver feedback / survey
Security culture	Driver security awareness	[1-5]	Driver feedback / survey
	Driver security commitment	[1-5]	Driver feedback / survey

3.6.2. Capture data for security performance monitoring

A key challenge of security performance monitoring is collection of reliable and relevant data, with reasonable effort. Fleet managers and logistics planners should discuss and develop means of data capture with truck drivers, company accountants, IT experts, and people responsible for trucking security. A company security plan should define rules for collecting and storing quality data on trucking security incidents and activities. The table below illustrates data fields and formats of the TAPA Incident Report Form that is used to collect data to the Incident Information Service (IIS).[6]

Table 3.5 Data fields and formats of TAPA Incident Report Form

Data field	Format	Data field	Format
Date of incident	DD.MM.YYYY	Cargo details	Written
Time of incident	HH:MM	Loss value	EUR
Incident category	Multiple options	Location of incident	Multiple options
Operating modes	Multiple options	Site of crime	Written
Description of incident	Writing	Route from	Written
Attempt	Yes / No	Route to	Written
Cargo category	Multiple options		

6 Annex G of this toolkit contains more detailed version of the IIS data fields.

3.6.3. Re-evaluate security plans & practices regularly

Continual and iterative process of risk management – where feedback is collected, analysed and considered in decision-making – is the key to improving risk management over time and staying ahead of criminals, stowaways and terrorists. Performance monitoring provides evidence for reevaluation and updating security plans and activities across all stages of trucking security management. Surprisingly high cargo theft losses, for instance, would suggest that the company management should revisit security plans and perhaps invest more time and money on proactive security measures. Performance monitoring indicates how security performance has changed after implementation of a new solution. This information helps managers to examine, compare and implement potential future solutions.

4/ ANNEX

4.1. ANNEX A. TOP SECURITY TIPS FOR TRUCK DRIVERS

https://ec.europa.eu/transport/themes/security/land_security/road-security-toolkit_en

4.2. ANNEX B. SECURITY PLAN

This annex outlines the essential elements for writing a security plan for trucking operations. This template uses the security risk management model introduced in Chapter 3.

A security plan is the cornerstone of secure trucking operations that sets the basis for a strong security culture and strong security practice. A company security plan should cover at least the following steps, themes and elements:

1. Allocate security responsibilities to competent and qualified persons who have appropriate authority and high motivation to carry out their security related tasks. Nominate the head of security, preferably a senior expert with strong skills and substantial experience in trucking security.

2. Assess security risks of trucking operations. Refer to Paragraph 3.2 “Assess Risk”. Involve key business partners – including shippers, freight forwarders, carriers, security service providers, and insurance experts – in the risk assessment, if possible.

3. Define measures to be taken to mitigate security risks in trucking operations. Refer to Chapter 3 of the ROADSEC toolkit keeping in mind specific requirements and needs of your company regarding key layers of trucking security management.

   - Design & planning;
   - Process control & visibility;
   - Assets & data protection;
   - Human resource management;
   - Business partner management;
   - Aftermath capabilities; and
   - Disruption of criminal activities.

   Consider also state-of-the-art technologies presented in Annex D “Freight transport security technology horizon.”

   Keep in mind applicable laws, regulations, standards, internal company policies when selecting trucking security measures.

   Study closely the security measures recommended or required by EU AEO, UK Border Force, TAPA and others, by consulting the Annex E “Existing freight transport security standards and good practices.”

4. If necessary, tailor Chapter 3 and/or Annex A to match the exact security measures and tips applicable to your truck drivers.

5. Organise appropriate training and awareness building among the drivers using materials particularly from Chapter 3 and Annex A. Consider hiring security trainers from the outside of your company or send your drivers to a trucking security course.

6. Establish communication and reporting procedures to collect driver feedback and help the drivers to report suspicions and crime incidents. Refer to Annex G "Security incident reporting forms" and Paragraph 3.6.2 "Capture data for security performance monitoring".

7. Create procedures for periodic evaluation and update of security plans and procedures. Consider recommendations of the Paragraph 3.6 "Monitor & Revise." Collect feedback from drivers and consider the drivers' needs and wishes in day-to-day trucking security management.

8. Ensure that only authorised people access information in the security plan on a need-to-know basis. Establish necessary cyber security safeguards to protect digital information as well.

Altogether, when designing security plans, managers should consider the model of Chapter 3, which guides them through the most important aspects and themes of the modern-day trucking security management. Use also Chapter 3 and Annex A – potentially tailored versions - of the ROADSEC toolkit to communicate key aspects of trucking security to truck drivers.

4.3. ANNEX C. TRUCK SECURITY CHECKLIST

Trailer unit

1. Rear door and seals
2. Floor (inside)
3. Side walls
4. Roof/ceiling
5. Front wall
6. Undercarriage
7. Fifth wheel area
8. Fuel tank
9. Tyres
10. Engine compartment
11. Cab
12. Windjammer

Tanker

1. Engine compartment
2. Tyres
3. Cab
4. Floor
5. Fuel tank
6. Storage areas
7. Bumper
8. Inside tank

4.4. ANNEX D

This Annex provides an outlook on state-of-the-art security technologies that are available for trucking companies. Note that the list of technologies is not exhaustive.

Category	Solutions / advanced features
Access control	• Electronic keys • Multi-factor biometric driver authentication (for example, finger print, facial features, and iris)
Locks & seals	• Automatic or slam-locks applications • Remote locking capability • Electronic seals with remote reporting capability
Alarms & detectors	• Panic alarm button • Alarm of curtain / door opening • Cargo compartment CO_2 sensors for detecting stowaways
Camera surveillance for trucks & trailers	• Rear-view and cargo compartment cameras • Motion detection capability • Powerful optical zoom (30x) • Internet protocol (IP) cameras for web connection • Ultra-high resolution (> 3840 x 2160) • High frames per second (> 30 fps) • Infrared (IF) view
Track & trace	• Vehicle and cargo unit trackers • Geofencing capability • Remote vehicle immobilisation capability
Awareness & response	• Multi-channel telematics (e.g., mobile phone and backup two-way radio communication) • Mobile devices and applications for finding secure parking places • Real-time and on-demand traffic information • Smart phones or watches to alert driver if a truck or trailer door is opened • Vehicle-based mist generators to make it difficult to thieves to select high-value items on-board
Data-driven driver selection	• Driver whitelists • Advanced recruitment processes

4.5. ANNEX E. EXISTING FREIGHT TRANSPORT SECURITY STANDARDS

Key references for transport security related governmental standards and good practices include the requirements in:

- the EU Authorised Economic Operator programme (EU AEO): https://ec.europa.eu/taxation_customs/general-information-customs/customs-security/authorised-economic-operator-aeo_en
- the SAFE programme of the World Customs Organisation: http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/frameworks-of-standards/safe_package.aspx
- those operated by Member States, such as the UK Border Force's accreditation schemes: www.gov.uk/government/collections/civil-penalty-accreditationscheme-for-hauliers

From the industry side, the TAPA global standards: https://www.tapa-global.org/industry-standards.html - cover both freight whilst being stored, TAPA Facility Security Requirements (FSR): https://www.tapa-global.org/industry-standards/fsr/download-section.html and whilst on the move, TAPA Trucking Security Requirements (TSR): https://www.tapa-global.org/industry-standards/tsr/download-section.html

These standards, consisting of a number of security levels, cover goods in a warehouse environment, either being stored or transiting through on route to a further destination, or being transported via a truck. The standards themselves lay down a set of prescribed security procedures to assist in the supply chain remaining safe and secure.

4.6. ANNEX F. SECURE PARKING RESOURCES

Following two EU initiatives, SETPOS and LABEL, the IRU took over the administration of TRANSPARK, www.iru.org/apps/transpark-app a database of information appertaining to the location and facilities at truck parking sites throughout the region. However, due to various issues, no real indicators have been maintained as to the security levels which can be found at these sites.

In an attempt to identify sites which offer security for trucks to park, as crime incidents reveal that the majority of theft from trucks occur in unsecure parking, EPSPORG http://www.esporg.eu/ and recently TAPA https://www.tapa-global.org/industry-standards/psr/download-section.html have both introduced a certification programme to identify and increase the security status of those participating in the schemes.

The European Commission commissioned a study on Safe and Secure Parking Places for Trucks, concluded in December 2018 https://ec.europa.eu/transport/sites/transport/files/2019-study-on-safe-and-secure-parking-places-for-trucks.pdf. The study proposes in particular a common standard, audit procedures and interfaces for booking systems.

4.7. ANNEX G. SECURITY INCIDENT REPORTING FORMS

The European Committee for Standardisation, CEN, has produced "Specifications for reporting crime incidents", EN 16352:2013-06 (2013). This Euronorm can be used as a security incident reporting template, across all EU (and CEN) Member States as well as across all companies operating in Europe.

On the security incident data collection and analysis front, TAPA maintains an Incident Information Service, IIS, and produces monthly, quarterly and annual reports, highlighting the changes it sees in crime trends. Reporting incidents is simple via the TAPA website https://www.tapa-global.org/intelligence/iis-data-resource/how-to-report-your-incidents.html

To assist in ensuring the correct category of criminal activities is used, TAPA has produced the following Glossary: https://www.tapa-global.org/intelligence/iis-data-resource/iis-key-glossary.html

4.7.1. Incident Category Definitions

Type	Definition
Hijacking	The use of force (armed or unarmed), threat or intimidation to kidnap the driver in order to take the vehicle
Robbery	The use of force (armed or unarmed), threat or intimidation in order to steal shipments/ cargo while employees, guards or drivers are present and coerced to allow access (open doors), hand over goods, hand over vehicle
Burglary	Entry to a facility (plant, warehouse, transportation hub etc.) with the intent to steal shipments/cargo, without confrontation with employees or guards (may or may not be present)
Fraud	Theft by deception; offense of deliberately deceiving another in order to damage them — usually, to obtain property or services from the victim unjustly
Theft	General Term for wrongful taking of property without that owner's wilful consent
Theft from Facility	Theft of complete shipment/cargo while being stored or handled in a facility (plant, warehouse, transportation hub etc.)
Theft from Vehicle	The stealing of shipments/cargo from vehicle (truck, van, lorry, trailer etc.), without any confrontation with the driver (driver may or may not be present)
Theft of Vehicle	Stealing of vehicle (truck, van, lorry, trailer etc.), – with the shipment/cargo/load, while driver is not present
Truck Theft	Stealing of vehicle (truck, van, lorry, trailer etc.), – without any load/shipment/cargo
Attempt	The act of trying to steal cargo/load/shipment unsuccessfully

4.7.2. Operating modes

Type	Definition
Forced Stop	Stationary or vehicle Roadblock; Running off road by another vehicle; Drive by shooting
Deceptive Stop	Bogus police roadblock / fake road works / Diversion from main route / Hitchhiker / Fake Accident / "Stuck" vehicles / "Bump and rob"
Violence & Threat with Violence	The use of force armed/unarmed, Threat to use force; extortion
Deception	Posing as customer / driver / warehouse employee – "around the corner" / Changing delivery details / fraudulent delivery or release documentation
Intrusion	Breaking & Entering For vehicle/Truck: "Jump up" / breaking door's lock or seal / slashing tilt curtain (driver may or may not be present) For Facility: Breaking and entry at a warehouse/logistics or company premises
Internal	Active involvement in the theft by employee/s or driver
Unknown	Operating modes details are unknown

4.7.3. Location Types

Type	Definition
En Route	While in motion/driving
Secured Parking	Customer or IRU Approved as secured parking
Non secured Parking	Public; Roadside; not approved by customer or IRU
Origin facility	Plant; Warehouse
Destination facility	Plant; Warehouse; Distribution
Road Transportation facility	Pickup/Delivery terminal; Hub
Aviation Transportation facility	Airside – Tarmac, apron, runway; Air Hub, Landside hangar or warehouse within Airport perimeter
Authorities 3rd party facility	Customs; Ground Handling authorities warehousing and handling facility
Services 3rd party facility	Broker; Forwarder; Handling provider warehousing and handling facility
Maritime Transportation Facility	Theft from ferry terminal/ port/dockyard facilities
Unknown	From ..... To ..... (origin & destination are required)

4.8. ANNEX H. ADDITIONAL RESOURCES

Further to this European Commission security guidance, advice on other matters relevant to road transport workers and security can be obtained from the following sources:

European Commission Directorate-General Mobility & Transport
Road Transport: https://ec.europa.eu/transport/modes/road_en

International Carriage of Dangerous Goods by Road
The European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR) published by the UNECE contains security provisions in Chapter 1.10: https://www.unece.org/trans/danger/publi/adr/adr_e.html
Rights and responsibilities of lone workers
EU legislation sets out a number of requirements in regard of lone workers and health and safety at work:
EU Rights at work: http://ec.europa.eu/social/main.jsp?catId=82

European Agency for Safety and Health at Work: https://osha.europa.eu/en

The European Agenda on Migration and Irregular Migration
Further information on the work of the European Commission to address irregular migration within the EU:
https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-migration_en