‘CART Security Guide’

CARGO AND ROAD TRANSPORT SECURITY GUIDE

PRODUCED IN COLLABORATION WITH

DIPS Distribution Industry Partnership Scotland

RHA

DHL

RSA

MOTORWAY BUDDY

NaVCIS

MAPLE

NOTICES

It should be noted, that whilst every effort has been made to keep information and guidance as general as possible, it has not been practical to provide specific links or references to international legislation for different regions/countries. As such where recommendations for wider reading have been made or references to legislation are cited, there is a bias towards UK based information. As such readers should refer to their own legal responsibilities and commitments where applicable.

DISCLAIMER

"The purpose of this publication is to provide insight in to the existing issues faced by industry, and the scale of the losses incurred to date, according to publicly produced statistics, and further to assist in minimising the possibility of loss from the risks referred to herein. It does not imply that no other hazardous conditions exist.

The contributors do not claim that the items included in this publication form an exhaustive list of your risk exposures, or that all potential risks and hazards have been identified.

The implementation of any best practice measures, already widely in use within the industry, is the responsibility of the reader or user of this publication.

Neither the contributing companies, associations, industry bodies, service providers nor any subsidiary or associated companies or any of its or their employees or agents has any obligation, duty or liability to any person relying upon this publication in contract, tort, for breach of statutory duty or otherwise or accepts any responsibility for the accuracy of data supplied by another party or the consequences of reliance upon it."

Foreword

Security is key to the success or failure of any organisation and is not just the responsibility of the Boardroom.

Security threats are continuously evolving. Who, 20 years ago would have anticipated that Cybercrime would emerge as one of the most significant threats to both personal and corporate security? And so simple for the criminal to carry out, from the comfort of their own home, anywhere in the world.

The true scale of cargo crime is difficult to fully ascertain. The harsh reality is it costs businesses millions of pounds every year, yet as an industry we remain inexplicably reluctant to tackle some of the pertinent issues head on which only conspires to increase the risk posed by cargo crime.

In 2002 John Abbott the then Director General of the National Criminal Intelligence Service said that organised crime was behind most incidents of lorry load theft. Organised crime is big business and it is well organised: it is market driven, flexible and resilient. It ranges across jurisdictions both nationally and internationally; it uses all the latest technology. It has a financial strategy through fear and the corruption of key people inside organisations. It has marketing, distribution and communications strategies.

The industry can make the criminal's life more difficult but it needs to be as well organised as crime already is. Not everything to do with tackling crime has to cost money. Information is also hugely valuable. Everybody has a part to play in reducing cargo crime. Remember, trucks are stolen whatever their load might be. Even a tiny share of this can spell disaster for an operator and negatively impact on profit, client goodwill and securing future contracts. Therefore, it is essential for operators to take security seriously and not treat it as an afterthought.

Working together in partnership is the key to tackling cargo crime. Many people have a part to play: those in Government, police, insurers, shippers, vehicle and security device manufacturers and those who operate and drive commercial vehicles. Such a partnership can have a positive impact on crime. The RHA Security Committee was established in 1959 and has been working with the police, insurers, manufacturers and a number of trade organisations over the intervening years to combat cargo crime. The Committee continues to have constructive engagement with the police to help identify, target and disrupt criminal activity against the haulage and distribution industry. The Forum also provides a platform for debate, intelligence sharing, trends and product innovation. The industry has done a lot to help itself, but each company should continue to ask itself searching questions.

The aim of this guide is to raise awareness of security throughout organisations, from the office cleaner to the Boardroom. All employees should be aware of the wide variety of threats which are not just physical and the common sense measures that can often be deployed to minimise them. Any organisation should prioritise security with the same focus as health and safety.

This guide is the result of input from an extremely wide range of highly experienced professionals from the transport industry, police and insurance industry. I would like to acknowledge the commitment and input from all those involved without whom it would not have been possible to produce this guide.

We hope you enjoy reading it and find it useful in your own business activities. Remember good security does not necessarily mean vast capital expenditure. Good management procedures and policies can go a long way to reducing your risk.

CHRYS RAMPLEY
MANAGER, INFRASTRUCTURE, SECURITY & BUSINESS AFFAIRS
RHA

Preface

17 years ago my father, Jim Maple, published a commercial vehicle security guide, with the aim of helping marine insurance underwriters to better understand how to secure a commercial vehicle.

When he wrote the guide he wanted it to be of benefit to the industry and not a commercial advertising platform.

The guide was distributed free of charge by AXA insurance to their network of brokers, it was also made available for other interested parties and stakeholders. The guide was very well received by the industry and was seen at the time to be a significant development in the fight against cargo crime.

Today, the cargo crime landscape has evolved to an extent that I felt the circumstances warranted the writing of a similar, if not more comprehensive document. Pertinently, the reason my father had assumed responsibility for writing a security guide was because such a resource did not exist, cargo crime and specifically commercial vehicle security was a misunderstood subject; whilst there are far greater resources available today they are not easily accessible or readily available in one place, perhaps as a consequence and in many respects, cargo crime is still not fully understood.

Like my father I feel that as a manufacturer and supplier of vehicle security solutions, we are well positioned to bring all this information together for the greater good of our industry; and perhaps make the commercial vehicle world, a safer, more secure environment.

Although Maple are commercially involved in the industry, we occupy a unique position. For more than 43 years, we have made it our business to improve the security of commercial vehicles. During this time we have worked closely with the logistics industry, marine insurance companies, vehicle and OE manufacturers, police, trade organisations and government bodies. It has enabled us to see the subject from all perspectives and gain a greater, well rounded understanding as a result.

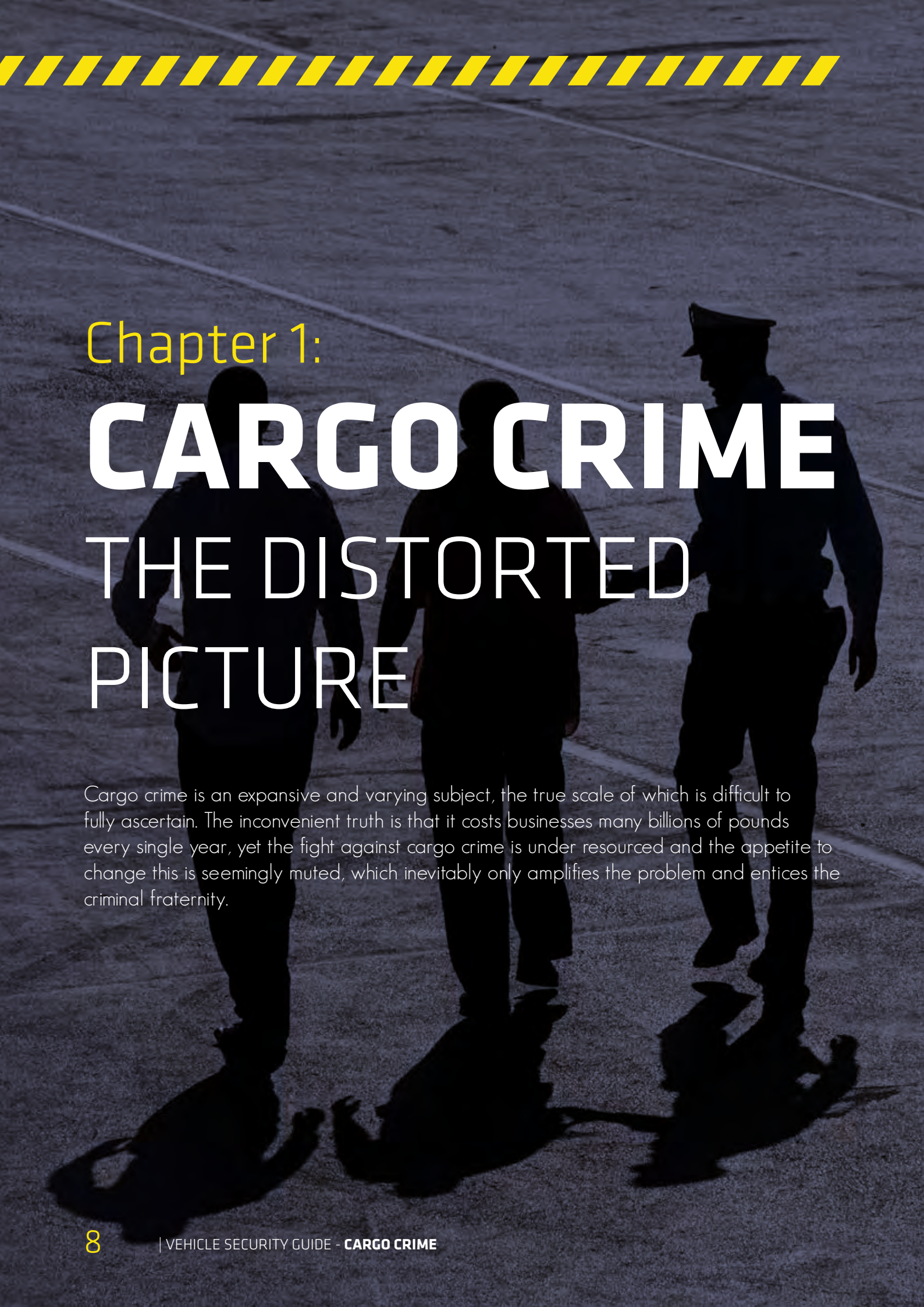
We have asked for involvement from other professionals and stakeholders within the industry, who like myself share a passion for fighting cargo crime. We wanted their insight, experience and professional opinion to ensure that the guide remained as informative as possible and provide a level of integrity that ensures the guide is not a commercial venture.

Finally, from a personal point of view, I do very much hope that the information provided here helps others to transport their goods in the most secure manner possible. If only a small percentage of the content included in this guide is beneficial, then I feel we will have achieved our objective and justified the resource and many hours invested in putting this guide together.

When you have worked in a particular industry for many years it becomes far more than just a job. It may have provided me a living but I also feel a level of responsibility; I gain a great deal of satisfaction when positive steps are made in combatting cargo crime. I'm therefore pleased, that with the support of our partners that formed the working committee on this project, we are able to distribute the publication without charge and put something back into a subject that is very close to my heart.

ALAN MAPLE
TECHNICAL DIRECTOR,
MAPLE

Contents



Chapter 1:
CARGO CRIME
THE DISTORTED PICTURE

Cargo crime is an expansive and varying subject, the true scale of which is difficult to fully ascertain. The inconvenient truth is that it costs businesses many billions of pounds every single year, yet the fight against cargo crime is under resourced and the appetite to change this is seemingly muted, which inevitably only amplifies the problem and entices the criminal fraternity.

The scale of the problem

Cargo crime is big business. It is widely reported that it costs EU member states €8.2 billion in the loss of goods per annum, an estimate based on a study conducted in 2007. FWI (FreightWatch International) have since attempted to revise this figure, and now estimate the actual value to be closer to €11.6 billion per annum.

With more than 31 million commercial vehicles on European roads, opportunities for cargo criminals are plentiful

The reality, however, is that these are only estimated figures. Despite positive progress being made by key stakeholders within the industry to better capture information, the true extent of cargo crime remains hugely distorted due to the scarcity of reliable data.

The lack of clarity is a direct result of inconsistent, sporadic reporting and misclassification of cargo crime incidents. Both TAPA (Transported Asset Protection Association) and FWI collate information via their members and supplement this with statistics from law enforcement agencies. The figures are, however, warped by underreporting and country bias, whereby only certain government agencies relinquish or even capture meaningful information.

Even data that is actively collated can show signs of inconsistency. For example, annual figures for 2015 from FWI, report 1,970 cargo crime incidents, compared to TAPA who report 1,515 for the same period. Significantly though, both parties did identify that incidents had been ominously higher than for the previous 12 months (a 30-40% increase). They also acknowledge that this figure is likely to represent only a snapshot of what is actually occurring, with an acceptance that only around 15% of all major cargo theft is recorded in the EMEA region.

€11.6 billion

estimated value of stolen cargo per annum

41% increase

increase in values of stolen cargo since 2007

€68,359

avergae loss in 2016 for cargo theft incidents (where loss reported)

THE CARGO CRIME OPPOURTUNITY

To those on the outside, cargo crime may almost appear to be a victimless crime. The occasional loss of goods incurred by large manufacturers and logistics providers may seemingly cause little harm, a view which is amplified by the low priority afforded to it by police authorities across Europe (and beyond). This latter point may be somewhat understandable, if not condoned, when you consider that higher-profile crimes which are deemed to be of greater importance to the general public compete for what is essentially a precious resource.

To those with a vested interest, who work within supply chain industries, the reality is, of course, far removed from this idealistic perspective. Cargo theft attracts the criminal underground, enticed by rich rewards, plentiful opportunities and relatively low-risk crime. Attacks are carried out by highly Organised Criminal Gangs (OCGs), who research, obtain inside information, target specific loads, and minimise risk at every opportunity.

For their part, criminals rarely resort to violence or the use of weapons; doing so would greatly raise the profile of cargo crime. There are of course exceptions, cases of hijacking, which although comparatively rare can result in physical attack or threats of violence to the driver (though it should be noted that this modus operandi tends to be reserved for the highest value heists). Cargo criminals are eager to remain under the radar as much as possible, keen to be left alone to exploit the unharvested opportunity that continues to be presented to them.

THE PATH OF LEAST RESISTANCE

In 2016 the average loss for cargo crimes classified as 'major incidents' topped more than €351,031, with the biggest single loss reaching a staggering €4 million (data recorded by TAPA EMEA). Single vehicle loads could carry goods to the tune of up to €20 million. If a bank held items to the same value on their premises you would need to defeat a plethora of sophisticated security measures to even gain access. In the event that you were successful the incident would be headline news, with CCTV footage plastered across various news outlets – the risk of carrying out an attack upon such a facility is huge. Commercial vehicles on the other hand may be protected by little more than a tamper-evident seal.

Companies the world over are happy to invest millions in IT and facility security 'Fences, cameras, alarms, motion detectors and security officers are all considered critical to the security of their company and product. An amazing truth in supply chain security however, is that these same companies put multi-million-dollar loads into a trailer driven by someone they do not know, whose identification they did not check, who may or may not actually work for the transportation provider they claim to represent and may not think twice about whether the load will arrive at its destination safely – or at all' (Cargo Theft, Loss Prevention and Supply Chain Security, Burgess 2013).

Every day, there are thousands of potential targets negotiating the road network from which criminals can select. So varied and readily available are these targets that criminals can afford to be selective in terms of which types of goods they target, when and where, capitalising on any vulnerabilities that exist in the carrying vessel.

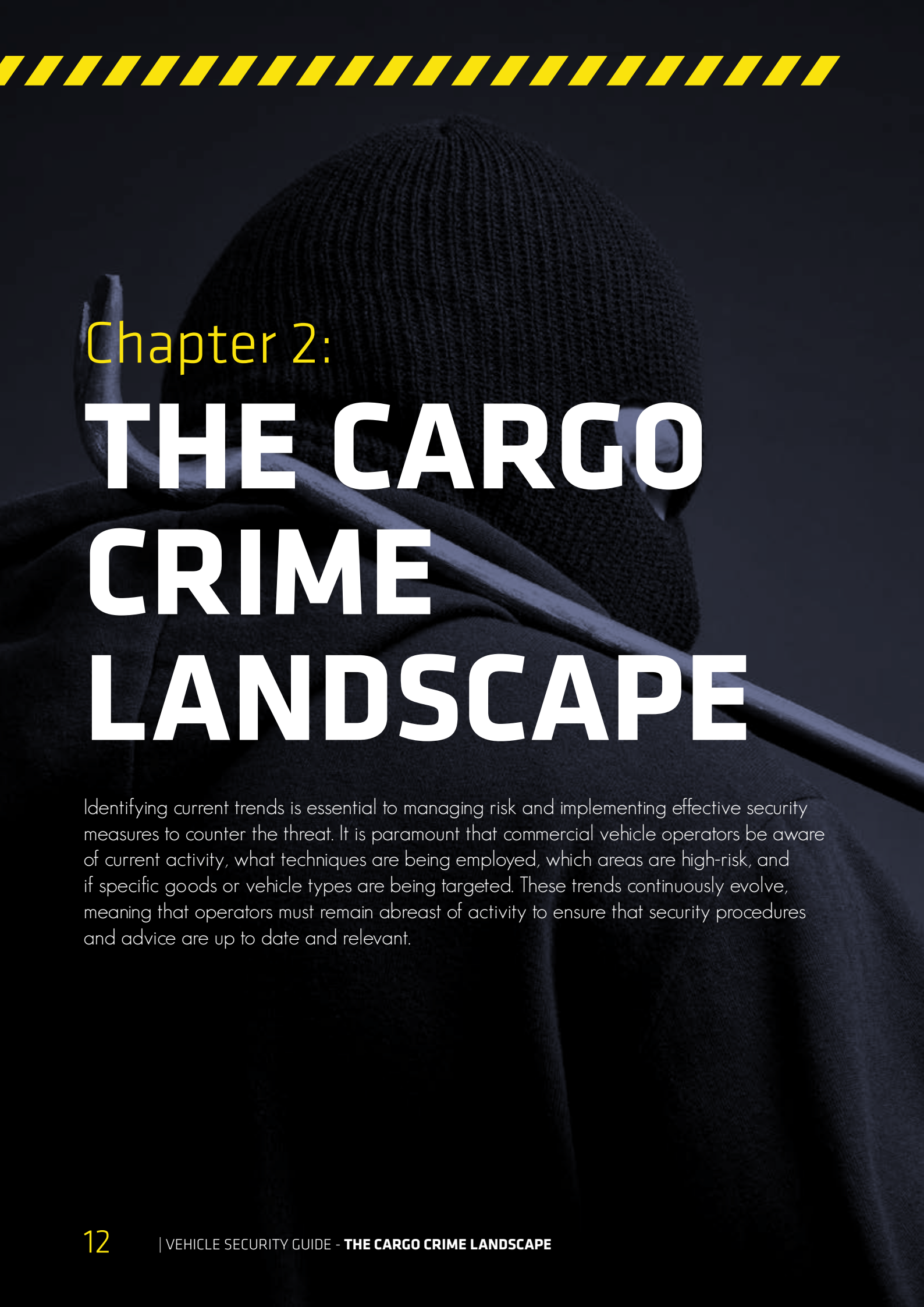
Ultimately, the risk undertaken by the criminal in carrying out cargo theft is low, opportunities are plentiful, and the barriers which they must overcome are, in many instances, far too basic – especially for such seemingly lucrative reward.

LACK OF DETERRENT

Cargo crime, in comparison to other offences, offers rich rewards with comparatively low risk. Drug trafficking, armed robbers (of facilities) and fraud, all carry lengthy sentences, conversely perpetrators found guilty of cargo crime may not even face imprisonment and almost certainly any conviction handed out is likely to be lenient. The following are only a selection of typical real-life examples of the light sentences handed out to cargo criminals, which does little to deter guilty parties or copycat crimes;

In 2013 a gang of thieves who conspired to steal 45 vans (durin a period of a few months) worth in excess of £500,000 were finally convicted. Two of the gang members who played significant roles were sentenced to just 26 months of imprisonment by Canterbury Crown Court.

In 2016, two men were caught by the police in the act of stealing a lorry worth £20,000. A 20-year-old man was sentenced to just six months of detention in a young offender institution, which was suspended for a year, with a two-month curfew and £340 in costs. His accomplice, who had a large number of previous convictions to his name, was also handed a lenient punishment, receiving a seven-month suspended sentence, 150 hours of unpaid work, and £570 in costs.



Chapter 2:

THE CARGO CRIME LANDSCAPE

Identifying current trends is essential to managing risk and implementing effective security measures to counter the threat. It is paramount that commercial vehicle operators be aware of current activity, what techniques are being employed, which areas are high-risk, and if specific goods or vehicle types are being targeted. These trends continuously evolve, meaning that operators must remain abreast of activity to ensure that security procedures and advice are up to date and relevant.

Scarcity of reliable data

'There is no simple way to provide a clear picture of the extent and nature of the theft of goods and commercial vehicles in Europe. In most countries vehicle and goods theft is not seen as a priority and few resources are given to collecting and analysing data on it.'

The last major study into organised commercial vehicle crime was conducted in 2007

This statement is taken from a 2007 study conducted by the European Parliament entitled 'Organised theft of commercial vehicles and their loads in the European Union'. The work covered in this paper went some way to providing a more detailed analysis of cargo crime, but was hampered by the availability of data. A decade on and the above statement is as true today as when it was written. Commercial vehicle crime is still underreported, with law enforcement agencies treating such incidents as a low priority.

The data that is available (collated by independent industry bodies) provides an overview of the current landscape. The information is, however, anecdotal; consequently, it is only indicative of the current level of activity, emerging trends, and hotspots of crime, and does not provide an accurate portrayal of all activity. Herein lies the conundrum, as the magnitude of the problem is difficult to ascertain, so to senior decision makers who must orchestrate the movement (and security) of goods in transit are doing so with only a partial view of what is actually happening.

40.7%

of cargo crime incidents occur in unsecured parking areas

€1 billion

estimated global rise in cargo crime value in 2016

74%

of cargo crime involves theft of goods from a vehicle/trailer

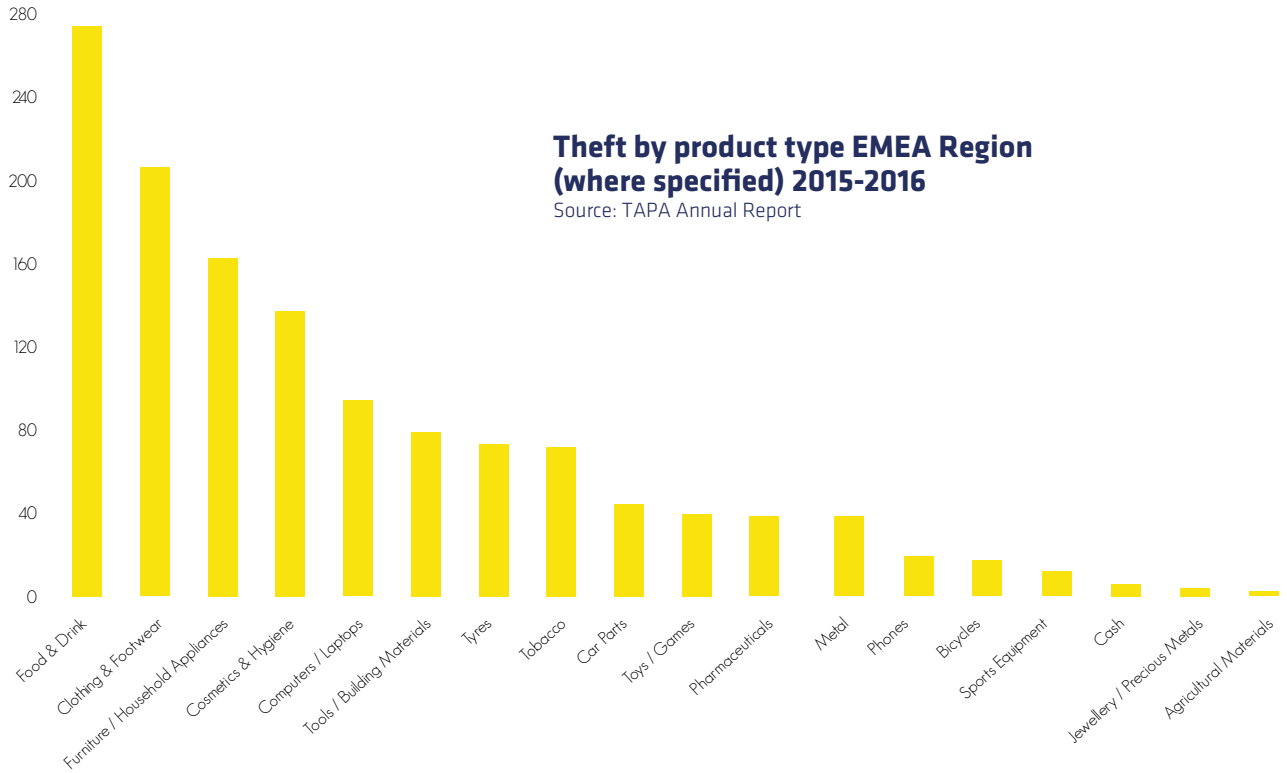
PRODUCTS AND MARKETS TARGETED

It is accepted that the vast majority of cargo crime is carried out by OCGs (Organised Criminal Gangs). It may be assumed, therefore, that there is a clear bias towards the types of goods being targeted and one may consider the most valuable loads to be most at risk.

Whilst it may be true that high-value goods, such as consumer electronics, and pharmaceutical goods are especially vulnerable, available evidence points to the fact that even low-value cargo, which may offer more readily moveable items and is almost impossible to recover, is increasingly at risk.

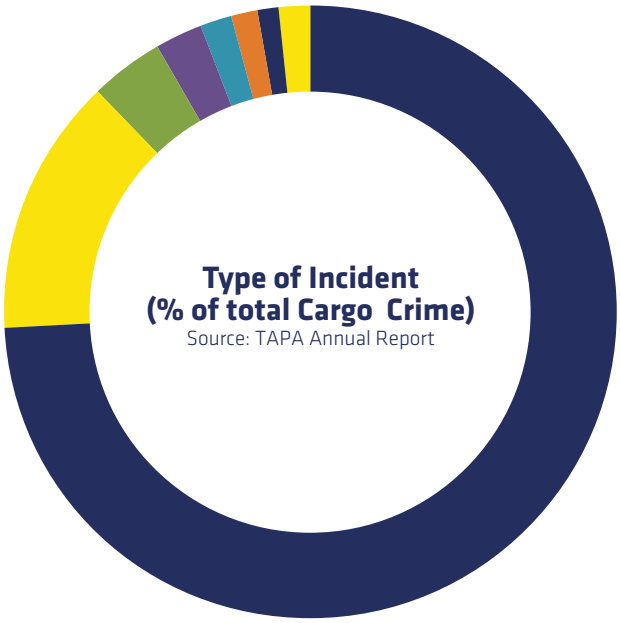
For example, in America, for four consecutive years, food and beverage has been the most stolen classification of cargo, a trend that is now also being replicated across the EMEA region.

STOLEN PRODUCT CLASSIFICATION



Theft by product type EMEA Region (where specified) 2015-2016
Source: TAPA Annual Report

TYPE OF INCIDENT

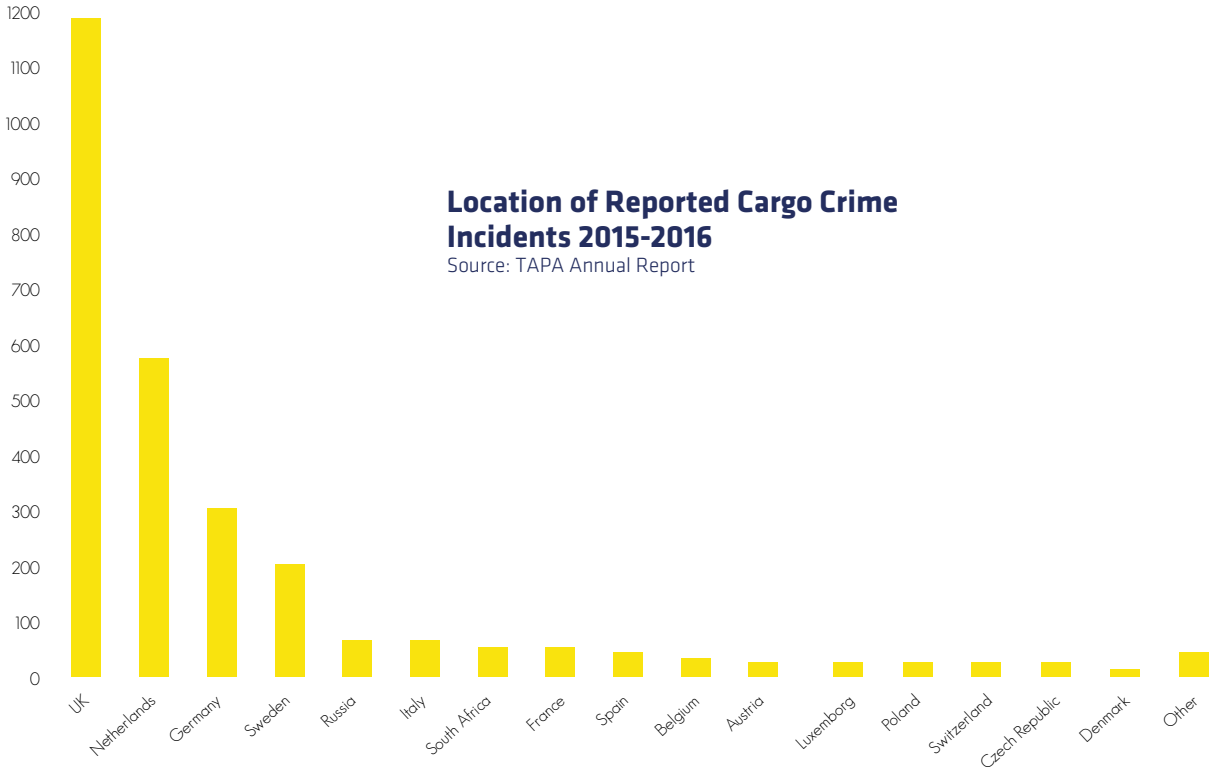


The picture of how cargo crime occurs is more consistent, with over 74.4% of incidents classified as theft from a vehicle or trailer (pilferage). Only 3.9% of incidents reported involve theft from a facility, reflecting the huge disparity between security measures employed in a warehouse or distribution centre and that of a vehicle, when goods are in transit, where the majority of incidents are committed.

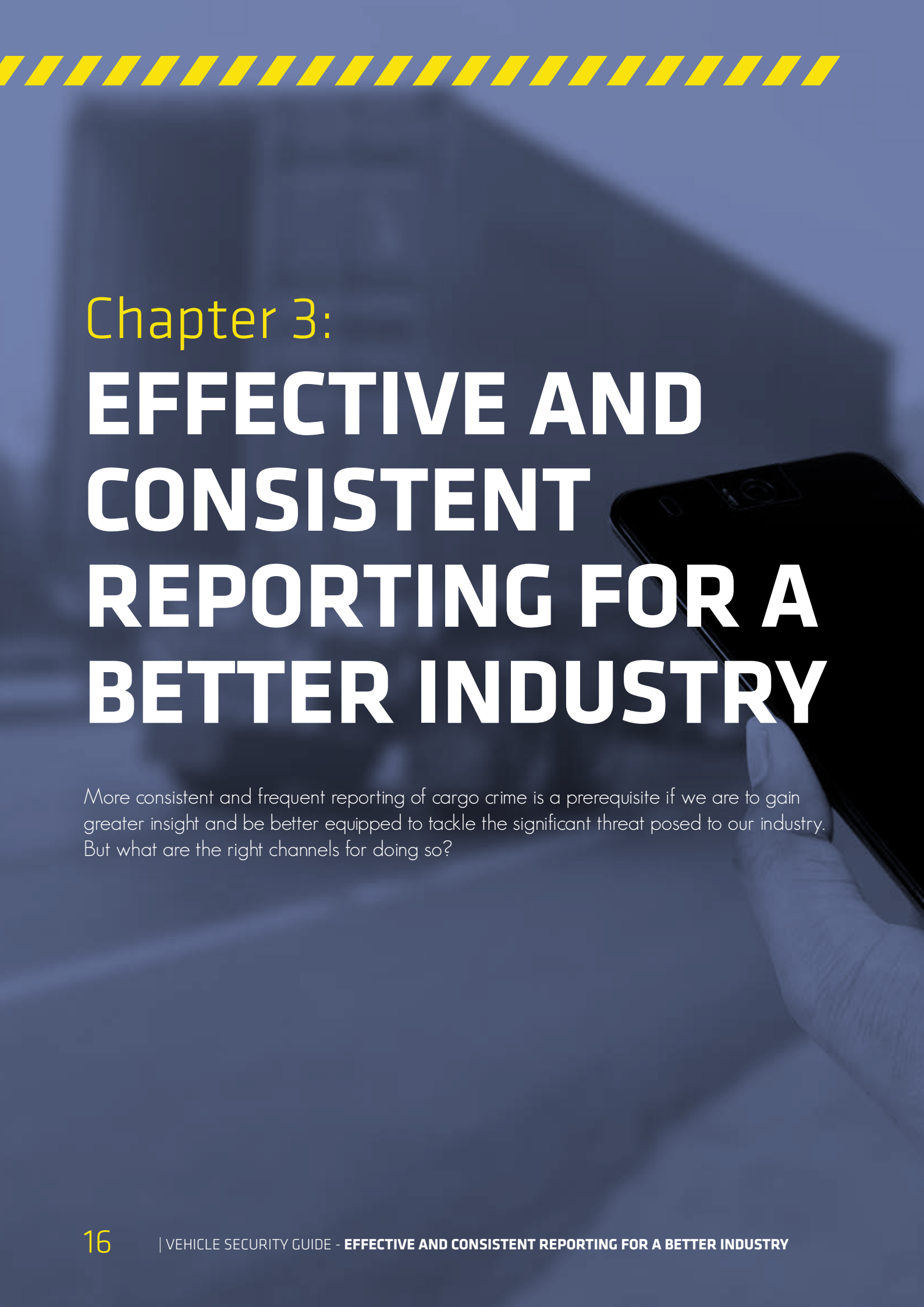
Theft from vehicle / trailer	74.4%
Theft of vehicle / trailer	13.4%
Theft from facility	3.9%
Hijacking	2.5%
Theft	1.9%
Theft from container	1.3%
Fraud	1.1%
Other	1.5%

CRIME HOTSPOTS

There is a strong correlation between incidents of cargo crime and the main European road transport corridor. The 'Blue Banana', encompassing the Netherlands, UK, Germany, Belgium, France and Italy, all feature prominently as cargo crime hotspots. Further analysis also highlights that a huge proportion of incidents, 40.7%, occur in unsecured parking areas, drawing attention to the significant importance of secure truck stop areas and rest areas, a fact that should be considered in route planning.



NB: It should be noted that the above statistics are skewed by the fact that not all regions are accurately reporting commercial vehicle crime data



Chapter 3:
EFFECTIVE AND CONSISTENT REPORTING FOR A BETTER INDUSTRY

More consistent and frequent reporting of cargo crime is a prerequisite if we are to gain greater insight and be better equipped to tackle the significant threat posed to our industry. But what are the right channels for doing so?

Reporting of cargo crime – historical problems

In the UK, since TruckPol was originally disbanded in 2012 there has been a void in the collation of intelligence surrounding cargo theft incidents. NaVCIS (National Vehicle Crime Intelligence Service) has since picked up the baton but during the intervening years it is estimated that the police were aware of some 40+ OCGs (Organised Criminal Gangs) involved in cargo crime, yet worryingly lacked sufficient resources or intelligence to prompt a meaningful investigation.

The dearth of reliable reported information is not a new phenomenon, and has plagued the industry over many years. There have been numerous attempts to rectify this situation. The aforementioned TruckPol had made significant progress before it was curtailed due to cuts in funding. TruckPol and RHA had also helped to support the TruckWatch initiative, which sought to raise awareness of cargo crime within the UK, providing alerts to hauliers and information about current activity. Despite some positive short-term results, the initiative was hampered by the familiar obstacle of a lack of funding.

Consistency is another major obstacle which continues to obstruct the effectiveness of reported information. There remains a large void in the number of police forces who actively report commercial vehicle crime incidents (to NAVCIS) and a lack of uniformity as to how it is classified (different forces use different reporting 'tags' to identify a cargo crime incident). Exasperated by a perceived black hole, as an industry, many incidents of theft and, indeed, attempted theft go unreported; those that are documented may not contain sufficient details (i.e. theft values, method of attack, type of vehicle, etc.), which only further distorts what is already a blurred landscape.

These problems should not be insurmountable. A clearer understanding of how incidents of cargo crime should be classified, together with a commitment to provide more detailed reports (from all stakeholders), would provide the platform for a much clearer and detailed picture, which could, in turn, be used to formulate a more effective strategy in combating cargo crime.

NaVCIS collate information of UK cargo crime incidents, they have successfully increased engagement from UK Police forces but currently around half still do not accurately capture freight crime incidents.

IMPORTANCE OF REPORTING

Consistent reporting is key to understanding the true scale of cargo crime. It helps us to understand further what is happening, where, how, and at what level. This information can also help to close the net on criminals, heightening their risk of capture and increasing the possibility of recovering stolen goods.

There are recent examples of how collaborations between business, police and cargo crime organisations have directly led to the arrests of suspects involved in the theft of goods from moving vehicles, demonstrating that a concerted, focused action yields results.

The information that is reported can provide vital insights into emerging trends and hotspots of activity throughout the UK and Europe. All stakeholders, therefore, have a responsibility to report incidents and share intelligence. A collaborative effort throughout the industry in reporting crime consistently and uniformly can only lead to positive action and a much safer, secure industry.

WHO IS RESPONSIBLE FOR REPORTING CARGO CRIME

It is, of course, an obvious answer: we all are. Drivers and employees have a responsibility to report any attempted, actual or suspected criminal activity to their manager. Managers, in turn, have a responsibility to cascade this information with their wider team, safeguarding both individual safety and the security of assets.

The more intelligence collated, whereby trends can be tracked and methods identified, the greater the potential that perpetrators will be brought to justice and the more we can do to combat crime. To this end, it is important that individual companies are clear about who is individually responsible and how incidents are officially reported to the police.

How to report incidents of cargo crime

BY PHONE

In an emergency you should always call 999.

For non-emergency enquiries or reports, call 101.

BY EMAIL

freight@navcis.pnn.police.uk

Alternatively, you can report cargo crime activity directly to NaVCIS (National Vehicle Crime Intelligence Service) via email; freight@navcis.pnn.police.uk

Based at the College of Policing near Coventry, the National Vehicle Crime Intelligence Service (NaVCIS) gather vehicle crime intelligence from UK police forces (approximately 50% of UK forces are currently reporting commercial vehicle crime data) and European law enforcement agencies. Having secured private funding, NaVCIS operate a full-time dedicated 'Freight Desk' to specifically target crime that effects the road haulage and freight transport industry in the UK.

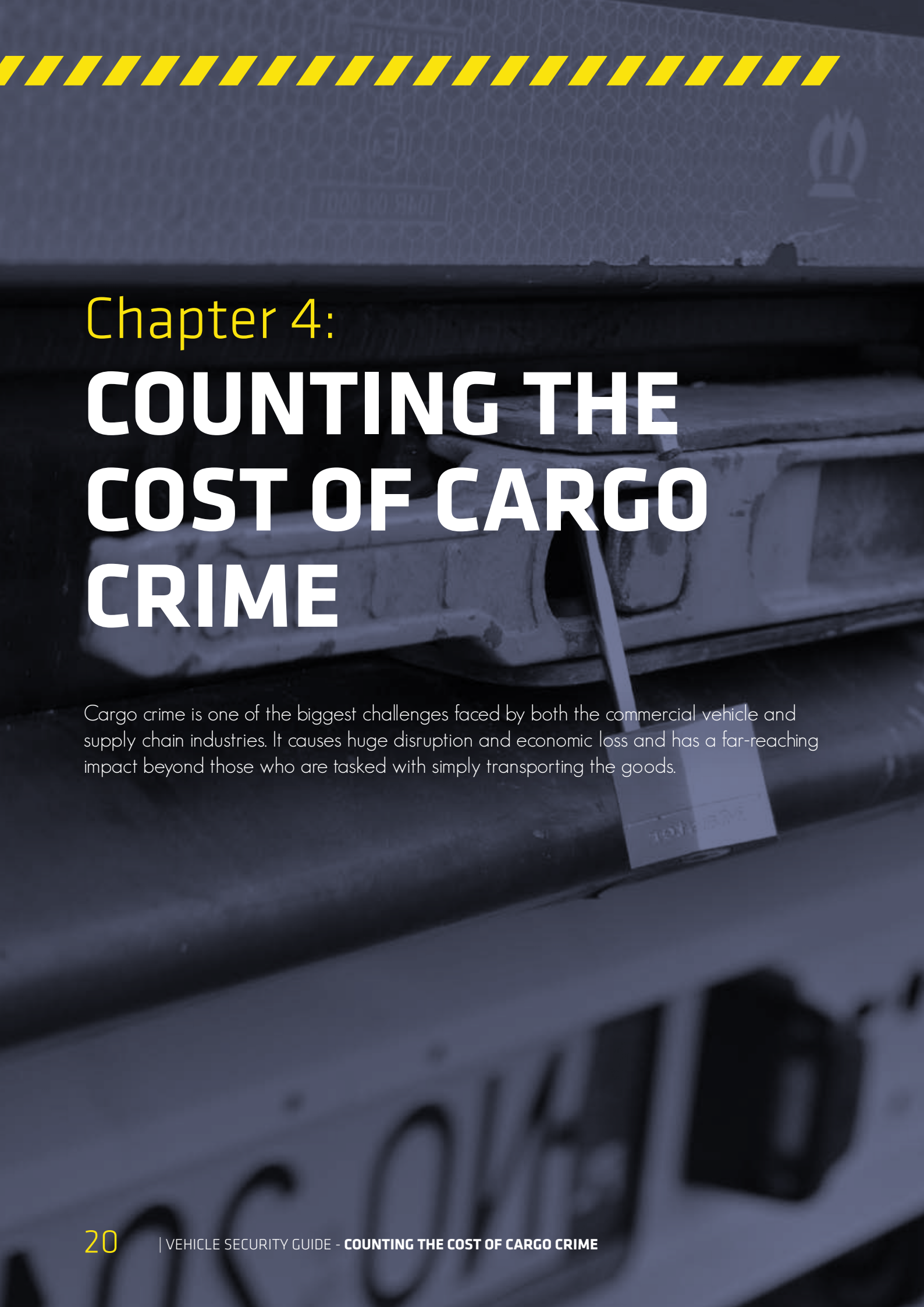
ANTI-TERRORIST HOTLINE

The UK's terrorist threat level has been classified as severe for more than two years (August 2014 - January 2017), which means that an attack is 'highly likely'. The attacks carried out in Nice (July 2016) and Berlin (December 2016), which saw a truck drive into crowds of innocent civilians, demonstrate the importance of remaining vigilant and alert at all times.

If you become aware of any unusual activity, no matter how seemingly insignificant, call the Anti-Terrorist Hotline immediately on 0800 789 321. All reports will be taken seriously. For further information, visit www.gov.uk/nactso.

Project Griffin, originally developed by the City of London Police, is an initiative for businesses which aims to advise and familiarise managers, security officers and employees of public and private sector organisations with security and counterterrorism issues. It seeks to increase engagement and encourage vigilance to combat the rising threat of terrorist activity.

Under the Project Griffin initiative you can get involved with free-to-attend awareness days and training sessions. The events are presented by trained police advisors, delivering a range of CT awareness modules. For further details, visit www.met.police.uk/projectgriffin.



Chapter 4:
COUNTING THE COST OF CARGO CRIME

Cargo crime is one of the biggest challenges faced by both the commercial vehicle and supply chain industries. It causes huge disruption and economic loss and has a far-reaching impact beyond those who are tasked with simply transporting the goods.

Financial cost to industry

We have already referenced estimated whole-industry costs of cargo crime (€11.6 billion per annum) and the fact that this may be nothing more than the tip of the iceberg. But what about individual per-incident costs?

The true cost of freight crime extends far beyond load loss values

TAPA (Transported Asset Protection Association) cites an average loss per incident of €29,741, though this value increases to €351,031 when considering only 'major cargo crimes'. These values are based solely on reported cargo losses, with no consideration of indirect or consequential loss; furthermore, only 43.5% of those crimes reported had an actual loss value attributed to them, thus distorting the overall average figures further.

In reality, the true financial burden must also account for the associated impact, including but not limited to:

- Cost of replacement goods and associated expedited charges
- Cost of repairing or replacing damaged/stolen vehicles
- Potential loss of business/contracts or even penalties incurred for late/missed deliveries
- Damage to reputation and brand – associated cost of stolen products in circulation
- Hire vehicle costs (whilst the vehicle is being repaired and/or the insurance claim is being settled)
- Shortfall in insurance settlement amount vs. cost of vehicle repair/replacement
- Insurance premium increase
- Potential fines for carrying clandestine persons (and cost of damaged or spoiled loads)
- Administrative and investigative costs
- Potential loss of jobs

In part, some of these costs are absorbed by the manufacturers, distributors and carriers but, ultimately, they are also passed on to the consumer, who perhaps unwittingly pays a premium for goods and services as a consequence.

SELF-EMPLOYED AND OWNER DRIVERS

Whilst the costs of cargo crime are, undoubtedly, damaging, many will view these as an unavoidable by-product of supply chain activity. For smaller businesses, tradesmen and sole traders the effects can be infinitely more harmful.

In the UK, some 4.69 million people are self-employed; accounting for more than 15% of the workforce, many of these individuals may be reliant upon a vehicle for their day-to-day business. In the event that they fall victim to vehicle crime, it is a direct attack on their livelihood: loss of tools/equipment, damage to vehicles, replacement costs, loss of earnings, and even the threat of a repeat attack (after the vehicle has been repaired and equipment replaced). Ultimately, such attacks could result in the bankruptcy of a company, which has far-reaching effects on the economy as a whole.

DECLINING WORKFORCE

There are intangible costs, too, which over time may have a more significant impact on road transport as a whole. In a sector that is already suffering from a huge driver shortfall, (the Road Haulage Association reports a deficit of 60,000 drivers, with an ageing workforce shedding another 40,000 annually), a potentially hostile working environment does little to improve the negativity surrounding the profession.

Indeed, drivers increasingly fear for their own safety, as the threat posed by persons attempting to gain entry to vehicles crossing borders grows ever more desperate and violent. In a survey conducted by Maple, more than 90% of drivers felt that clandestine activity posed a serious threat to their own personal safety – this is before even considering the far more intimidating prospect of incidents motivated by cargo crime that may involve hijacking and/or threats of violence.

The threat to drivers' safety may not be solely responsible for the lack of young people entering the industry, but it is yet another factor that is making it difficult to reverse this trend. As an industry we must also heed these concerns and seek to improve the conditions in which a driver is expected to do their job, from making provision for scheduled stops at secure parking locations to a safer and more secure vehicle in which to carry out their job.

THE RIPPLE EFECT

It would be easy to assume that the consequences of cargo crime affect only the profits of the already wealthy, but what about the wider implications? What other ripples are caused by the stone being thrown?

Cargo crime's promise of rich rewards and easy targets means that it is intertwined with the wider criminal fraternity. There are links to mafia, who are believed to be responsible for a high proportion of pharmaceutical cargo thefts (an estimated €30m cost per annum), and other notorious criminal organisations. Cargo crime may be nothing more than a 'cash cow' for criminal organisations; thus, the longer the fight is under-resourced and allowed to remain a low priority, the more it could be used as a vehicle to fund wider criminal activity.

FAQs

Q **Is there a standard for commercial vehicle security which I can use to demonstrate to my customers how seriously we value the security of the goods we transport?**

A TAPA (Transported Asset Protection Association) is a global organisation that unites manufacturers, logistics providers, freight carriers, law enforcement agencies, and other stakeholders with the common aim of reducing losses from international supply chains. TAPA have established Facility Security Standards (FSR) and Trucking Security Standards (TSR), which indicate that providers adhere to minimum acceptable security standards, including policies and procedures employed to maintain them.

There is no legal requirement to meet these standards. Members do not have an obligation to adhere to them, but by applying for certification they are demonstrating their commitment to providing a consistent level of security. TAPA standards are often referenced as part of contractual negotiations. For more information on TAPA, visit www.tapaemea.org.

Q **Would my insurers cover me for theft from my vehicle when parked in a lay-by if I fitted increased security?**

A This is subjective and down to each individual insurer and/or the type of goods being carried and/or whether the insured is a carrier or a cargo owner, with a fleet of owned vehicles. Generally, though, it is unlikely.

In short, carriers / cargo owners should exercise best practice and due diligence, regardless of the load being carried. It is as important to protect the asset (vehicle / trailer), safeguarding the employee sleeping in the cab and, of course, the goods. Ergo from an insurers perspective they would not advocate parking in unsafe, or unsecured locations irrespective of the security measures deployed.

Q **I am told that if I fit security on my vehicles my insurance premiums will reduce. Is this true?**

A Again, this is subjective, but in the vast majority of cases premiums will not be reduced. Insurers will not generally apply a percentage discount upfront for fitting a specific device, or being a member of a specific organisation. This is because, on the whole, risks are priced according to the claims history and potential loss exposure considering the nature of the goods and the operation as a whole. In addition, premiums would be priced competitively anyway, as the risk is either marketed across a number of insurers for them to quote on (e.g. a bidding process would keep premiums realistic based on the presentation of the risk by the broker), or if remaining with an incumbent insurer by negotiation on expiring terms.

Ultimately, by using security devices, being proactive via a risk managed approach, and acting as if no insurance was in place (or in other words as a "prudent uninsured"), then a business should suffer fewer losses, subsequently making it a more attractive proposition for insurers, and in turn keeping premiums at a fair level when compared to a business which is risk averse. Furthermore, some insurers will provide rebates of premiums on well-performing accounts or risk managed accounts at the end of the policy year to reward a client's efforts in loss prevention / risk reduction.

Q **What are the contractual and insurance considerations when moving goods along the supply chain?**

A It is important that stakeholders be clear about the terms and conditions under which goods are carried, as well as any terms of sale (or Incoterms for imports / exports in particular, to determine where risk and ownership in the goods transfers) and who is responsible for insuring the goods during transit.

Often, carriers do not insure the goods, only their liability for loss and/or damage to the goods, which in a large number of cases is not sufficient to cover the total loss, or value of the goods in the event of an incident. In the UK carriers tend to operate in accordance with industry standard terms such as those published by the RHA (Road Haulage Association), The FTA (Freight Transport Association), or BIFA (British International Freight Association); conversely international transits would be subject to applicable statute laws for the mode of transport concerned.

For international road transits between European countries such movements would predominantly be governed by the CMR Convention. All such conditions of carriage restrict the extent of a carriers liability using a weight based calculation in relation to the goods, though in the case of CMR it may be possible to break such limits, should "wilful misconduct" be proven. Cargo owners / manufacturers should ideally obtain marine cargo insurance, who would reimburse the agreed value of any lost / damaged goods in full, and then seek a financial recovery against the responsible carrier under subrogation rights. Some larger global companies may also opt to be self-insured, or operate with large deductibles, or within a captive arrangement.

Chapter 5:
CARGO THEFT AND SECURITY SOLUTIONS

The weakest point of the supply chain is that of goods in transit. Risk increases exponentially at the moment a vehicle leaves the relative safety of the depot and enters the uncontrolled environment of the road network. Goods are protected by various layers of security when in a warehouse or facility; it is a restricted zone which is naturally protected by bricks and mortar, people, procedures, and additional physical security. Once those same goods leave via a vehicle this shield of protection is instantly weakened, whereby they are now exposed to a host of unique, uncontrolled variables, a set of variables that contribute to a multi-billion-pound problem.

Exploiting opportunities

Cargo crime is nothing new – it dates back thousands of years. It started in Ancient Egypt when goods were transported from one village to another on camels.

When combatting freight crime it is important to develop a strategy rather than rely on any one single solution approach.

At night, when they stopped at watering holes, with the desert as their bed, bandits would come out of the desert under the cloak of darkness to steal loads from the camel's back. To combat this they invented wooden cages with primitive locks for protection. Some five thousand years later, have things really changed all that much? They have insofar as we have trucks instead of camels and truck stops instead of watering holes, but still the bandits come when no one is looking (The Big Blue Book, Maple, 2001).

The methods that 'bandits' use may have evolved, as have security and our approach to it, but still they seek to exploit the most obvious frailties within the supply chain. The vast majority of cargo crime occurs when the load is at rest and/or unattended, reflecting the fact that thieves are only too willing to take advantage of the vulnerabilities presented to them. Whilst misdirection and fraudulent activity may be less frequent in comparison, their very existence is also down to exploitation of an opportunity born out of vulnerability (see Chapter 14 for more information). It is therefore important to note that there is no silver bullet for effective cargo security; rather, it should be a multi-layered approach.

As individual stakeholders in the supply chain industry, we must all take responsibility for combating this threat, doing more to learn, educate (our colleagues and employees), share information and, ultimately, take sufficient precautions and instil preventative measures to counter the threat at large.

SOFT-SIDED VEHICLES AND CURTAIN SLASHINGS

Curtain-sided vehicles remain a popular choice for hauliers, offering greater operational flexibility in terms of loading and unloading, increased efficiency and, of course, a cost advantage over their hard-sided counterparts. However, soft-sided vehicles are, by design, enormously vulnerable; somewhat remarkably, they are also used to carry high-value loads on an astonishingly frequent basis.

High frequency of attacks

A large proportion of commercial vehicle crime is apportioned to OCGs (Organised Criminal Gangs); however, even within this context, opportunism remains a factor. In many cases, criminal gangs will specifically target certain vehicles and/or loads, often acting upon inside information to lead them directly to the desired haul. Equally, criminals may be stealing to order but acting without any knowledge of what individual vehicles are carrying. It is common practice for thieves to speculatively slash a high number of curtain-sided vehicles in a localised area until such point they find their desired load.

Curtain sided vehicles are particularly susceptible to attack

A typical example occurred in Germany during November 2015, where at various motorway rest areas, soft-sided trailers were specifically targeted. On some evenings, more than 40 trailers had their curtains slashed but no goods taken, whilst subsequent attacks led to the theft of tyres, cosmetics and computer hardware. The police noted that it was apparent that the perpetrators were seeking very specific products, a trend that was repeated a number of times.

In common with the overall picture of cargo crime, the full scale at which curtain-sided vehicles are attacked is incomplete. Incidents often go unreported, particularly if no goods are actually stolen, whilst those that are reported are not specifically classified as curtain incidents. However, industry intelligence points to the fact that it is the most prevalent of all incidents. A large UK-based haulier claimed that they can suffer up to 850 curtain slashes a month, costing them upwards of £21,000 in repair bills alone (Commercial Motor, 2010).

It is not just theft against which hauliers must guard. Any vehicle crossing the border is subjected to the threat of clandestines attempting to gain entry to load areas (see Chapter 16 for more information). It is understandably more difficult to secure curtain-sided vehicles; nevertheless, there are measures that can be employed to significantly raise the level of security on this type of vehicle.

SECURITY SOLUTIONS FOR CURTAIN-SIDED VEHICLES

Prohibiting access to a curtain-sided vehicle is, for obvious reasons, an inherently difficult task. Their flexible, moveable 'walls', which could be 'attacked' at any given point, make the task of effectively securing them an arduous one.

ALARM SYSTEMS

One may assume that an alarm system could offer a good level of security for a curtain-sided vehicle, but traditional methods of sensing infiltration are unreliable for such applications. Door-opening contacts offer only limited protection, and sensors which are often used on other vehicle alarm systems are unreliable in a curtain environment due to unstable conditions (i.e. sensors usually work by detecting sudden changes in air movement, temperature or motion, all of which are conditions wholly more irregular within a curtain-sided vehicle than those offered by a hard-sided vehicle). Furthermore, the way in which soft sided vehicles are loaded and so tightly packed and the potential for metallic loads which further hinder sensors, mean even positioning detection sensors in such a way so they can gain full sight of the load area, let alone withstand damage when loading and unloading, is incredibly difficult. Factor in the requirement for 0% false alarms and a difficult task becomes almost impossible – certainly at a cost effective price.

For an alarm to work effectively in this environment, there must also be provision for detecting any cutting of the curtain (which could occur at almost any physical point), which given the aforementioned problems of how a curtain sided vehicle is loaded, is again a significant challenge.

Some vehicle security providers have previously designed, and in some cases manufactured alarmed curtains. These were generally curtains with thin electrical wires attached to the inside and in turn connected to a vehicle alarm. In the event that one of the wires was cut, the alarm would sound, and in some cases send a message to a monitoring station. Although over time, improvements were made to reliability and robustness of the attached wire, the high cost, difficult maintenance and relatively small demand meant it was not a viable solution.

It is not to say that alarms are impossible for such applications but their reliability (and suitability) is questionable. Detecting or preventing unauthorised access to a curtain-sided vehicle is, therefore, much more difficult to achieve – difficult, though not impossible..

REINFORCED CURTAINS

Specialist slash-resistant curtains can be fitted to provide protection against knife or cutting attacks. Typically, they are manufactured from Kevlar or incorporate galvanised steel wires bonded to the interior surface. In the event that a knife does penetrate the surface, the steel wires block any further dragging or movement of the knife. Such curtains can readily be sourced either from new or for a retrofit, providing an immediate uplift in security without compromising flexibility.

Reinforced curtain material

TIR SEALS

Load access monitoring systems for curtain-sided vehicles provide dual protection against theft and unauthorised entry. Replacing the traditional bond cord with a tamper-proof, air-pressurised version, any subsequent damage or cutting of the TIR cord will trigger an alarm or covert notification. The TIR cord is paired with a rear-door electronic seal to provide a visual load status, offering a clear notification in the event of unauthorised access.

Detecting the initial attempt to penetrate a curtain-sided vehicle offers one of the most effective security measures that can be employed on soft-sided vehicles. It enables drivers or operators to identify a potential security breach at the earliest opportunity and take action immediately.

In-cab notification of curtain opening

HARD-SIDED VEHICLES & LOAD AREA ATTACKS

Seventy-four per cent of cargo crime incidents involve the theft of goods from a vehicle/ trailer; a significant proportion of these occur when a vehicle is parked or is at rest (often at an unsecured parking location).

On hard-sided vehicles or trailers the most obvious point of intrusion and, therefore, biggest vulnerability is that of the load area doors. Despite the high-value loads that commercial vehicles carry, a remarkably high number of road transport companies still choose not to specify locking solutions.

The Home Office estimate that approximately one third of lorries arriving at the UK border do not have even basic standards of security in place, a statement that takes on even greater significance when considering that research shows that perpetrators will invariably move on to softer targets if they cannot defeat security measures in under two minutes.

For operations in which vehicles do not have scheduled stops and are carrying lower-value goods it is common for hauliers to use nothing more than a basic tamper-evident seal, which does not prevent access to the vehicle. Reliance upon such measures is ill-advised, particularly with the emerging trend of theft from moving vehicles (see Chapter 13 'The Romanian MO') and the heightened risk posed by clandestines attempting to conceal themselves within vehicle load areas. More pertinently, carriers must address whether the physical level of security that they are employing is offering an adequate level of protection and whether it is fit for purpose (the use of tamper-evident security seals is covered in more detail in Chapter 6).

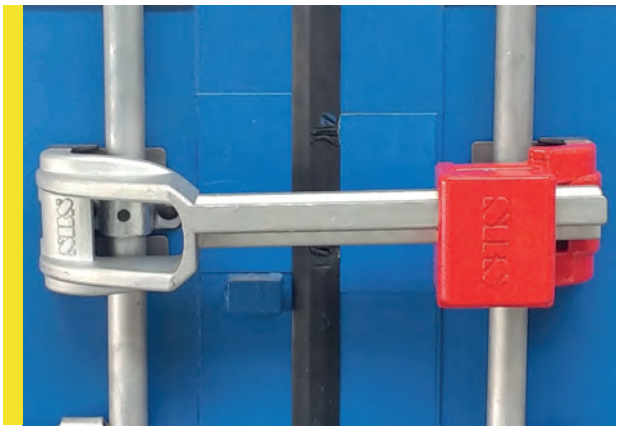
Containers can be particularly challenging to secure

SHIPPING CONTAINERS

Though multimodal sea containers share similar characteristics with trailers, they provide a more complex security conundrum. As it is common practice for goods to be shipped in containers that are not owned by the freight forwarder, the methods that can be used to secure the container itself are limited.

Because the container is owned by a 3rd party, security solutions that are available for containers, are in the main designed for temporary use, thus when the assignment has been complete the device can be removed and returned to the owner. But how can you be sure it will be returned? Who is responsible for doing so? And will it be in good condition, without any missing parts (such as padlocks)?

In addition, if using a locking based security application the consignor must also consider how they are going to control access. How will keys be distributed? To whom? When? Are all locks in circulation accessed with the same key profile and if so what happens in the event one becomes lost or stolen?
In most cases, these logistical challenges are never quite overcome and consequently, it is common for shipping companies to rely on the use of seals.



A range of mechanical locking solutions. From top to bottom; (1) Container Lock, (2) BDL (Barndoor Lock) and (3) the Alligator Lock.

LOCKING SOLUTIONS

There are various considerations and factors that can influence the type of load area security system that you require. Firstly, there are practical considerations such as what products are being carried and the nature of operation (i.e. trunking, multi-drop, international transport). There are external factors such as the routes that you plan on using (Are there hotspots of activity? Are you likely to encounter clandestines attempting to board your vehicle? Are there secure parking areas en route?) and the perceived level of threat to the goods being carried; additionally, there are internal factors such as who requires access to the load area and when.

These factors or influences are key to determining what is the most appropriate level of security for your vehicles.

MANUAL LOCKING SOLUTIONS

At the more basic end of the vehicle security spectrum are manual locking solutions. Usually they are mechanical, key operated devices and typically could include a padlock based option. These manual systems require the driver or other employee to physically apply or operate the lock before the load area is protected. Typically the locks will fit around exterior locking bars by clamping them together or by bracing the doors against the chassis.

Manual locking systems offer a good visual deterrent and offer a basic level of protection against forced entry but as an exterior mounted application they are potentially more susceptible to attack. As with mortice locks on buildings, they are also entirely reliant upon an individual using them correctly and locking them each and every time the load area has been accessed.

AUTOMATIC LOCKING SOLUTIONS

The next step in terms of functionality is the automatic or slamlock application. Ensuring that doors are locked as soon as they are closed or handle is secured, provides a considerable improvement to goods in transit security, especially for multi-drop operations.

Unlike some manual solutions, slamlock applications are permanently mounted to a vehicle, thus it mitigates any ambiguity of whether the security system is being correctly employed. Operators should also consider the specification of the lock itself and the level of security it affords, for example internally mounted systems (on the inside of the load area) will typically provide greater protection in comparison to their externally mounted counterparts, as they are naturally more difficult to manipulate or attack. Depending on the type of door furniture and lock mechanism, you may also opt between single or multi-point locking applications.

Consideration as to how a locking system is powered should also be factored in when deciding upon the most appropriate solution. Pneumatic solutions inparticular are capable of generating significant force in powering locking cylinders and deliver excellent reliability, it also ensures that on trailer applications, locks can still be operated when not connected to a power source. Alternatively self-powered solutions may offer advantages over vehicle powered systems, thus in the event of flat vehicle batteries or electrical failures, access to load areas can still be achieved.

A range of automatic locking solutions. From top to bottom (1) Maple Freightlock fitted to shutter, (2) Internal view of high security locking bolts, (3) Maple's integrated locking and sealing solution, Integritas).

EMERGENCY ACCESS

It is inevitable that at some stage access keys/fobs will be lost or even stolen. In the case of automatic solutions, drivers may, on occasion, lock their keys inside the load area. It is therefore important to consider what would happen in such scenarios; after all, if you have specified a security solution that is anywhere near effective it should not be easy to force entry. Therefore, in such instances, how, if at all, are you able to access your goods?

The more sophisticated access control systems feature single-use emergency access codes, which can only be accessed by authorised persons. Once inputted, door locks will be released to enable temporary access, before reverting back to their standard operation.

Similarly, what happens if a driver becomes locked inside the vehicle, particularly in a chilled or frozen environment? Ensure when you are specifying such applications that a driver always has a means of releasing the locks from inside the load area; make sure staff are aware of how to use the internal release and/or instructions are clearly displayed on the inside of the vehicle.

Q **Is it possible to operate multiple locks operating from the same key? What happens if a key is lost or stolen?**

A It is perfectly possible to offer matched key and barrel sets, though in the event that a key is lost or falls into the wrong hands, this has obvious security implications for all units featuring the same key. Many security systems can be provided with key plans, which have the capacity to enable individual access but with master keys that access all units. Electronic or RFID systems can provide user-friendly key management software, which enable lost or stolen keys to be deleted and replacements issued.

Q **Is it possible to source vehicle locking systems that do not require mechanical keys?**

A Some operators may prefer to retain greater control over who has access to their goods and when. Linking a security application directly to a vehicle's telematics system can provide remote access control, so load areas can only be accessed under controlled conditions; thus, the driver has no means of access to the vehicle. Alternatively, locking systems can be controlled via the use of rolling PIN numbers or access codes, which can be issued securely to authorised personnel.

Q **I have heard about geo-fenced locks, which can only be opened when at an exact address. Is this possible? And how reliable are they?**

A This is perfectly possible but operators should exercise caution. Such systems are reliant upon an available GPS/GPRS signal. Consequently, if this is not available or a signal becomes blocked then you will not be able to gain access to the vehicle. Furthermore, vehicle doors could be unlocked before they are physically inside the secure delivery point, leaving vehicles temporarily vulnerable. An alternative approach is to have a layered system, where access is enabled when a vehicle enters a certain area, but a secondary key fob or access code is still required to unlock a vehicle.

Q **How can I best secure vehicles which are not directly owned by me? Can you purchase temporary, removable security devices?**

A There are a number of specific removable locking devices that can be used to secure vehicle doors. Container door locks, which clamp external locking bars together and are secured with the use of a padlock provide a temporary/removable option (see page 32 for more detail). Kingpin locks can also help to guard against unauthorised movement or coupling of trailers and are, again, temporary solutions that can be moved from one unit to another.

Q **If my driver is stopped at customs and the driver has no key to open the door, how can they gain access?**

A Some access control security systems provide users with the ability to unlock vehicles remotely or via the use of single-use emergency access codes. Discuss available options with your vehicle security provider; however, it is important to allow for such incidents, especially with more stringent border controls coming into force.

Guarding against load theft

Prevention (not detection):
There is no substitute for robust, physical security equipment to protect your vehicle and its cargo. When specifying locking and security products, they should be appropriate and fit for purpose, minimising the risk of misuse or abuse..

Swiss Cheese Model:
When developing security procedures, build layers. Security can be likened to multiple slices of Swiss cheese, stacked side by side, in which the risk of a threat becoming a reality is mitigated by the differing layers and types of defence which are "layered" behind each other, i.e. lapses and weaknesses in one defence do not allow a risk to materialise, since other defences also exist, to prevent a single point of weakness.

Security Policy:
Establish and implement an in-transit security policy with clear procedures for the driver to follow. Ensure that this policy is included within induction training and is well communicated.

Operations:
Consider operational policies, such as if drivers are allowed to stop (if so, where), keys to be removed, doors to be locked and sealed (and never accessed en route), and if a driver should remain with his load at all times.

Delivery Policy:
Be clear about what paperwork is required. Who is responsible for unloading and should the driver be in full view of the unloading process at all times? Drivers should be vigilant and mindful of deception techniques. Ensure that you are delivering to the exact location specified (for further details see Chapter 14).

Define Risk:
Define and assess the risk involved in individual assignments/contracts. Factors such as geographical locations, routes, time of delivery, number of persons involved, and nature of the goods being carried should all be considered.

Accountability:
Ensure that all required stakeholders are aware of their responsibilities, understand the requirements, and agree to action and/or abide by them; ultimately, they must agree to be accountable for individual responsibilities (shippers, carriers, clients, etc.).

Evolution:
Continuously review procedures for effectiveness and relevance. Remain abreast of current threats and update procedures accordingly if necessary.

Fit for Purpose:
Ensure that you are using the right equipment for the job in hand. Are the vehicles suitable for the goods being carried? Moreover, have you specified adequate and appropriate security equipment?

Cargo at Rest is Cargo at Risk:
A high percentage of load theft is carried out at weekends and from vehicles parked at (unsecured) truck stops or rest areas. Do not leave vehicles loaded unnecessarily, and carefully plan where your drivers are authorised to stop.

Chapter 6:

TAMPER-EVIDENT SECURITY SEALS

Tamper-evident seals provide an indication of whether unauthorised or unexpected access has occurred. They are widely used within the transportation industry, coming in various guises with varying degrees of security and effectiveness. The key question is one of appropriateness: are the seal and the management of the system appropriate for the application? Is the seal required for detection or prevention?

Tamper-evident seals

Tamper-evident seals are widely used on various applications, from fresh produce to chemicals, duty-free carts to shipping containers. They are intended to detect intrusion or contamination, either accidental or deliberate, providing unambiguous, non-erasable evidence in the process. They are not intended to delay or repel unauthorised entry.

'Barrier seals', which are part 'lock' and part 'seal', offer a rudimentary level of security but are, by no means, a substantial level of protection against theft and are often a compromise rather than an effective solution.

Furthermore, tamper-evident seals are open to manipulation and misuse; thus, they are susceptible to being opened and then resealed without detection. This is not to say that seals are ineffective. If used for their primary intention and managed correctly they are perfectly adequate. However, as with all security considerations, it is vital to be clear about what you are realistically expecting to achieve.

Plastic or bolt seals, whilst indicative of load integrity, offer little to no protection of goods in transit and provide no tangible accountability. Once again, they are wholly reliant upon individuals using them correctly, and arguably raise many more questions than they resolve. Was the vehicle locked? Who has access? Was the seal applied correctly (or did it merely appear to be)? Was the load area accessed en route, when and by whom?

In short, ask yourself if your existing procedures are adequate, suitable and managed effectively. Are they fit for purpose? Procedures and, indeed, legislation for the transportation of goods where product integrity is paramount, such as fresh produce and pharmaceuticals, must also be carefully considered when developing security protocols.

105 Different methods

for potentially defeating a seal without detection

244 Different seals

all of which were tested and defeated

90% of seals tested,

could be defeated in less than 3 minutes

The above statistics are the result of a study conducted by the Vulnerability Assessment Team of Argonne National Laboratory

SECURITY SEAL STANDARDS - ISO 17712

ISO Standards are a set of requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose. ISO 17712:2013 establishes uniform procedures for the classification, acceptance and withdrawal of mechanical freight container seals. It provides a single source of information on mechanical seals which are acceptable for securing freight containers in international commerce.

Specifically, to conform to the standards, a seal must be assessed for physical strength (the seal is then classified as either a High Security, Security or Indicative Seal), seals must be designed and constructed with tamper-indicative features that generate tell-tale evidence of tampering, and manufacturers must also be audited for security-related business processes.

It should be noted that a high-security seal (as classified under ISO 17712) can generally be removed with bolt or cable cutters. Moreover, the standard does not make any reference to (or take into consideration) electronic seals or integrated locking systems, which, by design, offer a heightened level of protection and integrity.

C-TPAT – CUSTOMS TRADE PARTNERSHIP AGAINST TERRORISM

C-TPAT is a voluntary public-private sector partnership programme operated by CBP (US Customs and Border Protection); its primary objective is to work with the trade community to strengthen international supply chains and US border security.

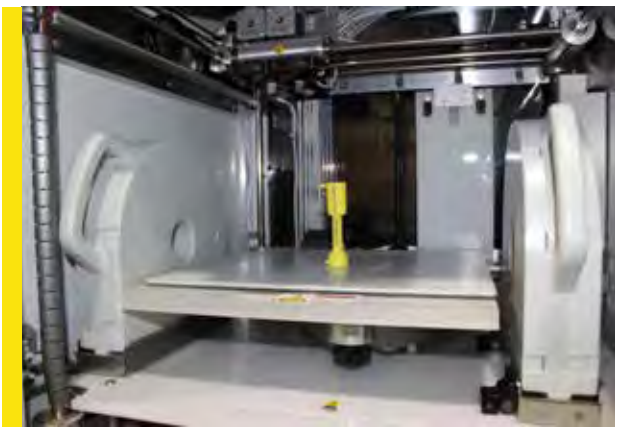
When members join C-TPAT, they agree to work with CBP to protect the supply chain, identify security gaps, and implement specific security measures. Applicants must be able to demonstrate plans to align security throughout the supply chain. In exchange, members benefit from reduced inspections at the port of arrival, expedited processing at the border, and other significant benefits, such as penalty mitigation.

C-TPAT's security criteria states that "...a high security seal must be affixed to all loaded containers bound for the U.S. All seals must meet or exceed the current ISO 17712 standards for high security seals."

EMERGING TREND – USE OF 3D PRINTING IN CARGO THEFT

Exploiting rapid advances in 3D printing technologies, criminals are now able to produce replica 'High Security Cargo Seals'. This sophisticated tactic is already known to be in use, with documented cases revealing how counterfeit seals displayed the exact identification number as the original. Visual inspections reveal very little and in many cases it is only after the seal is removed that the theft is discovered.

To safeguard against this threat, carriers should consider alternating the colour of security seals used and making periodic changes to suppliers to counter the threat of copied/cloned seals. Issuing seals in random order, so that criminals are unable to anticipate specific seal numbers, and ensuring that logs are maintained and audited regularly will also help to deter such attacks (G4S intelligence bulletin; 2016).



3D Printers are being used to produce counterfeit seals

Types of Seal

INDICATIVE SEALS

The first level of tamper-evident seals is generally classified as an 'Indicative Seal'. They are designed to be tamper-evident, such that if any attempt has been made to access a vehicle or container, the seal will need to be broken. Available in various guises or designs, they are a low-cost, low-security option and should be used only where a chain of custody is required, rather than as a preventative security measure. Basic indicative seals do not require any application or removal tools.

In utilising such seals, operators should be mindful that in the event that they are broken, they provide no information or details about when or where the intrusion occurred. They are also open to manipulation and misuse, with their entire success dependent upon an effective and well-communicated procedure regarding their correct use (e.g. when they are applied, checked and removed, how details are documented, and who is responsible for doing so).

BOLT SEALS AND CABLE SEALS

Offering a more robust and higher level of physical security than that of their plastic counterparts, bolt and cable seals usually require specialist tools for removal. Seals in this category would typically adhere to the classification of 'High Security Seals' under ISO 17712; however, they also share many of the same characteristics as indicative seals, such as the lack of detail concerning removal and reliance upon an effective, well-managed procedure.

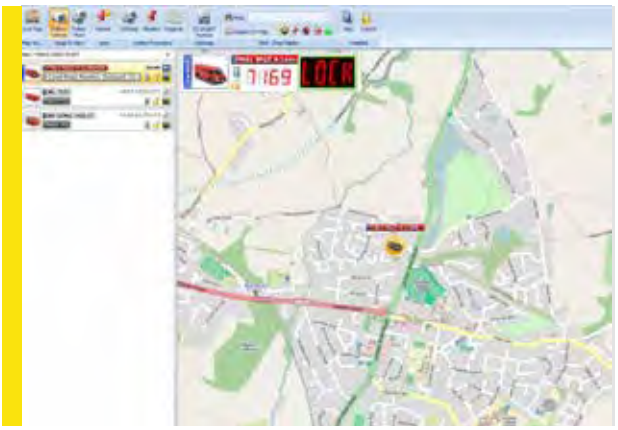
By design, bolt cutters are required to remove the seal; consequently, the level of physical protection that they provide is limited. Furthermore, there are a host of techniques that can be employed to manipulate a seal to give the impression that the seal remains intact but has, in fact, been removed (be it for criminal purposes, terrorist activity or people smuggling).

ELECTRONIC SECURITY SEALS

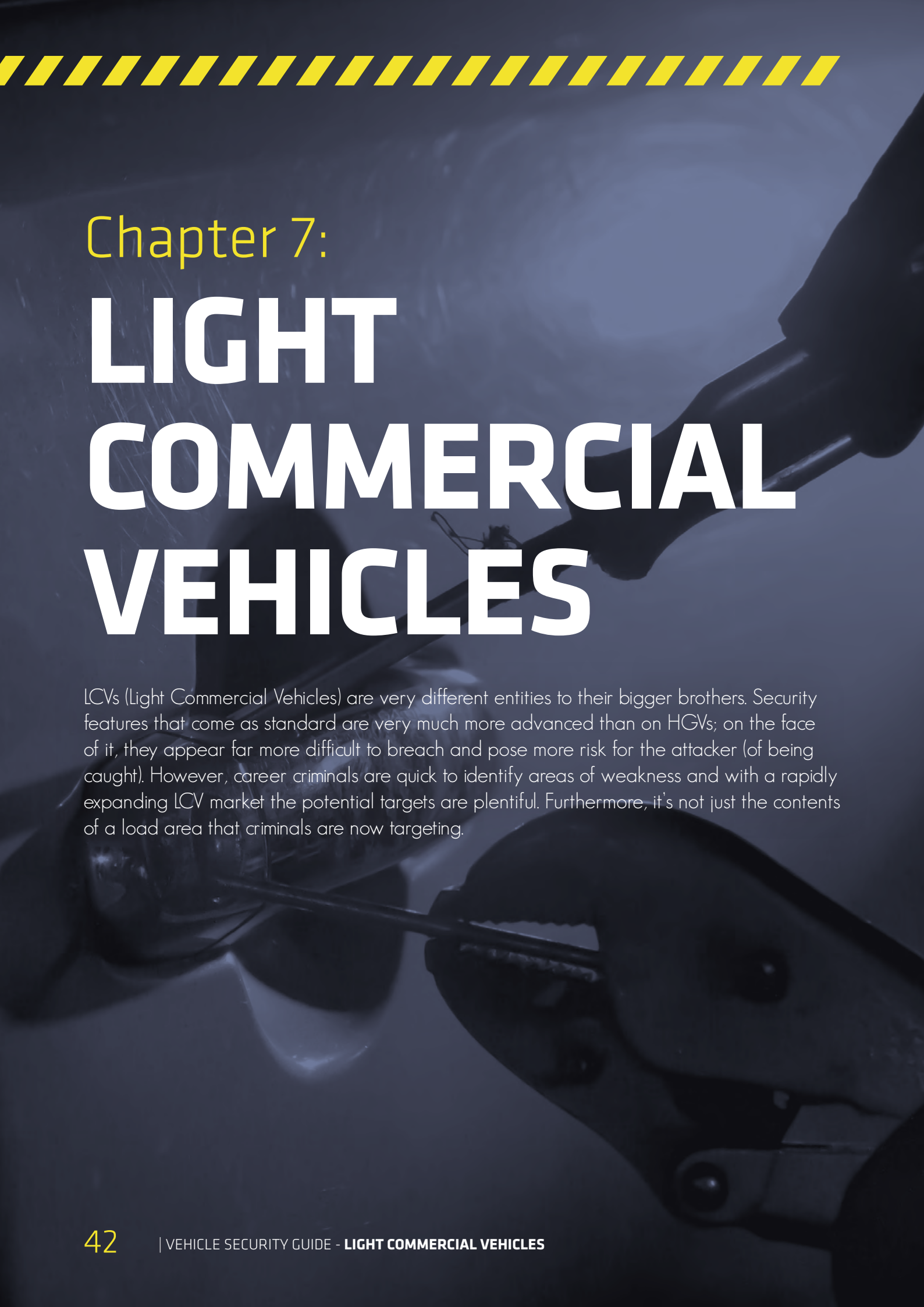
Designed specifically for the road transport industry, electronic seals are designed to streamline and simplify load integrity procedures. As a permanently mounted system, the seal itself is reusable and offers full audit trail capabilities, so operators are able to identify all door and seal activity.

Some systems integrate with locking applications to provide a complete end-to-end security system, preventing unauthorised use (via PIN number identification or a key fob) and protecting against forced attacks. This approach also allows operators to opt for an automatic system, such that each time a load door is closed it instantly secures the doors and provides a new randomly generated seal number. Audit trails for these applications are also more intrusive, revealing who has carried out individual operations when and where.

Electronic seals offer an alternative to basic sealing applications, providing more insightful information, whilst also attributing accountability of goods whilst they are in transit. They can assist in removing areas of ambiguity and blind spots that may otherwise exist within the logistics process, whilst offering a more flexible and appropriate methodology for road transport operations, particularly those involved with the movement of sensitive, high-value or perishable goods.



Electronic seals can help to improve load integrity, providing accountability and transparency of operations. Top to bottom (1): Maple Barndoor Freightlock, (2) Integration with telematics for real time door status and remote access control (3) Maple Integritas fitted to shutter door



Chapter 7:
LIGHT COMMERCIAL VEHICLES

LCVs (Light Commercial Vehicles) are very different entities to their bigger brothers. Security features that come as standard are very much more advanced than on HGVs; on the face of it, they appear far more difficult to breach and pose more risk for the attacker (of being caught). However, career criminals are quick to identify areas of weakness and with a rapidly expanding LCV market the potential targets are plentiful. Furthermore, it's not just the contents of a load area that criminals are now targeting.

The resurgence of a Forgotten threat

It was a battle that was seemingly won – the theft of vehicles had reached a 48-year low. Statistics in 2014 revealed that the number of vehicles stolen was down 70% in 10 years. But criminals are now hitting back, exploiting new techniques to overcome manufacturers' security systems to illicitly access and steal vehicles. The trends are now in regression.

LCV registrations are predicted to increase 88% by 2035

Back in the dark days of the 1990s, vehicle theft peaked at more than 700,000 per annum. It triggered a response: in 1998 the EU issued legislation making the fitting of electronic immobilisers mandatory on all new cars and LCVs. It was the catalyst for bucking the trend of vehicle theft, as of 2014 just 0.2% of the 36 million vehicles on UK roads were stolen.

That good work is now under threat, as thieves have discovered techniques that enable a vehicle to be stolen without a key. The crime initially appeared to be isolated to high-end cars, which were, in all likelihood, being stolen to order, but LCVs are also increasingly falling victim. Vehicles with keyless ignitions or that do not require mechanical ignition keys are often most at risk.

Keyless theft techniques

OBD PORT (ON-BOARD DIAGNOSTIC) ATTACKS

The majority of modern vehicles are supplied with an On-Board Diagnostics port.

It is designed to allow vehicle technicians access to the status of the various vehicle subsystems. They provide real-time data in addition to a standardised series of diagnostic trouble codes, which allow rapid identification and remedy of any malfunctions within the vehicle.

The same port can also be used by garages and locksmiths to produce replacement keys in the event that an original is lost or broken. Unfortunately, this same method is being exploited by criminals to unlawfully take vehicles by simply programming a replacement key (using a laptop or specific device sourced easily via the Internet), bypassing the OE immobiliser and, thus, gaining full control of the vehicle without ever needing an original key, all achieved within a few short moments.

LOCK PICKING AND MANIPULATION

The picking of locking cylinders on vehicles was another threat seemingly resigned to the annals of history.

Firstly, locking mechanisms and cylinders were made more secure, meaning that coat hangers are no longer effective tools when breaking into vehicles. Furthermore, technological advances such as the aforementioned legislation for immobilisers and remote central locking meant that key barrels have been phased out, with the exception of the override cylinder on the driver's door.

Targeting the most popular models of van, thieves have devised techniques that can overcome the driver's door cylinders, often overriding central locking in the process. Without any specialist tools, thieves can quickly defeat the OE locking cylinder. In most cases, all that is required is a screwdriver to directly attack the barrel and release the locking mechanism or basic hand tools to twist the locking cylinder around until it releases the vehicle's central locking. This method provides easy access to the load area, thus making additional (secondary) locking systems vital to LCV security.

Criminals are utilising technology to bypass OE immobilisers

Typical example of an OE locking cylinder that has been attacked

Cab area security

OBD lock protectors prevent unauthorised use of the port

OBD PORT PROTECTION

The conundrum for manufacturers and, equally, van owners is how to restrict access to the OBD port.

It is not feasible to isolate the port or block it permanently; it is, after all, there to enable easier maintenance of the vehicle. In time, the OBD port could be relocated, though perhaps that could be counterproductive.

In the meantime, OBD protection devices, which restrict access by encasing the port in secure housing or prevent unauthorised use of the port by effectively immobilising its use, are effective measures to combat keyless, electronic vehicle theft techniques.

Installation of an anti pick replacement locking cylinder

OE LOCK REPLACEMENT

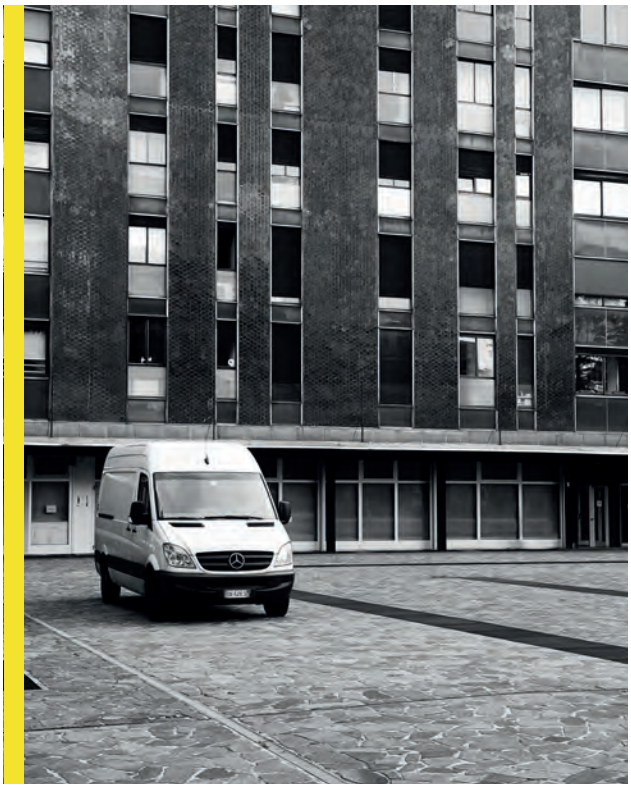
Once thieves have identified a weakness in a particular vehicle, the spread of that technique and its speed of adoption are akin to a virus.

A cost-effective solution to counter attacks on the driver's door barrel is to replace the existing cylinder with a bespoke, anti-drill, anti-pick alternative. Coupled with an outer protection bezel, it blocks and deters this increasingly common method of attack.

Merely the presence of such preventative measures is maybe enough to deter thieves from even attempting to break into a vehicle, especially when there is a plethora of other similar defenceless vehicles to target.

Panel van load area security

The logistics industry has evolved dramatically over the past two decades. Shopping habits, the commercialisation of the Internet, and changes to the way in which consumers receive and demand their goods have had a direct impact on the landscape of the road transport industry.



LCV ownership has increased by 29% in the last 10 years, with a shift towards ever-increasing home deliveries and a surge in demand for next-day and even same-day delivery in the home shopping market. Furthermore, utilities and service providers are more varied and numerous in their scope; thus, the demand for support of these networks increases, too. The flexibility that LCVs afford means that these trends are all contributing to an anticipated 88% growth in this vehicle type by 2035.

The increase in panel van registrations and the further expected rise mean that criminals can be more selective in their targets, whether that is led by vehicles that offer the least resistance or by the potential 'haul'. In addition to the techniques discussed earlier, where criminals exploit technological loopholes within a vehicle, there has also been a marked increase in physical attacks upon vehicles, from cutting of bodywork and the manipulation of OE locking mechanisms to aggressive prising of doors, all of which reinforce the importance of increasing load area security to provide a more comprehensive barrier against attack.

1st

Ford Transit most frequently stolen UK vehicle

2nd

Mercedes Sprinter is next on the list of stolen vehicles

38%

of stolen LCV's are never recovered

SLAMLOCKS

Traditional slamlocks are an old favourite amongst van owners and operators. Originally developed in the 1980s, as the name suggests, once the door is slammed shut it automatically locks. "The first mechanical slamlock that we engineered was a bespoke design for a utilities company who had been experiencing an astonishing amount of opportunistic theft of expensive equipment from unsecured vans," recalls Alan Maple of commercial vehicle security specialists Maple. "It soon became apparent that this was not a problem experienced by the one operator in isolation. Slamlocks were quick to be universally adopted by both insurers and the industry."

More than 30 years later, the humble slamlock is still a popular choice, particularly for multi-drop operations. The choice is, of course, a little more plentiful. Mechanical key versions are still widely available, whilst electronic offerings, with the ability to delete lost keys and enable emergency access (in the event that keys are locked inside) provide greater flexibility.

It is an important consideration that the majority of slamlocks are designed for convenience and reassurance, they do not necessarily provide additional protection against forced attacks. However, specialist slamlock applications, primarily reserved for sensitive or high value cargo operations are available. Utilising RFID technology, integrated locking and sealing applications, provide a host of enhanced features, including but not limited to;

- Heavy-duty, internally mounted, high security locking cylinders
- Automatic electronic sealing
- Audit trail (detailing who, when & where vehicle doors have been opened)
- Remote lockdown capabilities (lock and unlock vehicles via telematics system)

From top to bottom; (1) Mechanical key operated slamlock (2) Covert electronic slamlock (3) Maple's LCV Freightlock IQ, which integrates electronic sealing and high security locking

DEADLOCKS

Another van security staple is the manual deadlock. Providing an extra locking point to any door, van deadlocks are completely independent of the existing manufacturer's locking mechanism, so even in the event that a thief may have acquired the ignition keys or bypassed central locking, access to the load area is still restricted.

Deadlocks are a very popular addition and remain one of the most effective security measures that you can employ on a panel van. However, it is important to remember that as a manual option they are only as effective as the user themselves, as failure to physically lock the doors will render them defenceless.

ARMOURED LOCKS

Exterior-mounted, armoured shell casing locks offer an alternative to deadlocks. They usually feature an angled body which is designed to deflect direct blows from a hammer. Its interlocking rear body prevents the doors from being crowbarred or leveraged apart.

Its exterior-mounted position and heavy-duty appearance provide an effective visible deterrent, which, in some instances, may be enough on its own to deter thieves, who will simply move on to a target with less resistance.

PROTECTION PLATES

With so many panel vans on the market, thieves are quick to discover vulnerabilities in a manufacturer's design. In some instances, they may target central locking wires that will release doors if cut. They may identify and attack weak points of bodywork in order to override locking mechanisms or manipulate the OE lock to mimic the action of a key.

Bespoke security plates provide protection to weak points on a vehicle, surrounding, encasing or protecting the vulnerable area and repelling targeted attacks.

VEHICLE EQUIPMENT THEFT

Theft of on-board vehicle equipment is not a new phenomenon. In the 1990s it was the car stereo; with the dawn of the new millennium it was the portable sat nav. Theft of such items conformed to the stereotypical profile of opportunistic theft: the culprits happy to make a quick buck by moving the stolen goods on in the local pub. Today's perpetrators are a little more savvy, their prey a little more surprising.

Security solutions for vehicle equipment

CATALYTIC CONVERTER THEFT

In 2008, with the price of precious metals at a peak and the onset of a crippling credit crunch, the theft of catalytic converters soared. In just a three-year period, thefts were reported to have more than doubled; in some areas, incidents increased ten-fold.

On the surface it may seem a strange target but each device typically contains precious metals, namely platinum, palladium and rhodium, which, in turn, command a high resale value. Thieves primarily target vehicles with a high ground clearance, making panel vans particularly susceptible. For fleet owners, who may fall victim to multiple thefts in just one evening, this is not only a costly problem but also hugely inconvenient, impacting upon service levels and delivery schedules.

Particularly, dexterous criminals can remove a catalytic converter in under a minute; once removed, the vehicle cannot be driven, with repair bills running anywhere up to £3,000. This is before indirect costs are factored in, such as loss of revenue, hire costs, insurance excess, increased premiums, and even loss of business.

SPARE WHEEL THEFT

Another trend that has been on the increase is that of spare wheel theft. For panel vans, the spare wheel is usually stored on the outside of the vehicle, leaving it exposed and vulnerable to quick and easy removal by unauthorised persons. Costing up to £200 per tyre, spare wheels can represent a lucrative haul for the would-be-thief and an expensive headache for the transport manager.

Many fleet operators have resorted to storing the wheel inside the load area, which, in turn, impacts upon load capacity, or even removing the spare completely and storing in the depot, which has obvious repercussions in the event of a flat tyre.

SECURING EQUIPMENT

For high-risk vehicles/equipment, consider security marking items. Marking kits usually consist of a virtually indestructible sticker, marking fluid or electronic devices. It makes assets less attractive to thieves, as they are more difficult to move on. The risk of detection is greatly enhanced and the possibility of recovering stolen equipment for the owner is greatly improved.

There are also a range of engineered security applications that can be employed to further protect exposed equipment. Spare wheel guards (usually vehicle-specific) prevent unauthorised lowering of the tyre or removal until the protection device is unlocked. There are a host of catalytic converter security systems, ranging from warning alarms to physical clamps for the emissions control device, as well as vehicle-specific devices that prevent access to the catalytic converter itself (such as bonnet locks on the Mercedes Sprinter).

Guarding against LCV and van crime

Always Lock Your Vehicle:
It might seem obvious but ALWAYS lock and secure your vehicle. You can have the most secure locking solution available but if you don't use it correctly it's nothing more than a fashion accessory.

Protect the Load Area:
Arguably, the wisest investment that any van owner or operator could make is that of an additional security lock on load area doors. The biggest draw for a thief is your load area (more specifically, its contents), so protect it and make it as difficult as possible for criminals. Deadlocks and armoured locks provide a cost-effective physical barrier to forced attacks on your vehicles.

Education, Education, Education:
Educate and train your drivers as to what is expected. If a driver only plans to leave a vehicle for a few minutes, e.g. to de-ice windows, carry out a delivery or stop for fuel, vehicles should still be secured – thieves need only but a few moments. Ensure that drivers are trained to lock doors each time they leave the van and make them aware of the consequences of not doing so. Security is only as strong as the weakest link in the chain.

Keys Are Key:
Key theft is a common method utilised in vehicle crime, so ensure that keys are always stored in a safe place, be it at the depot or when vehicles are at a driver's home address.

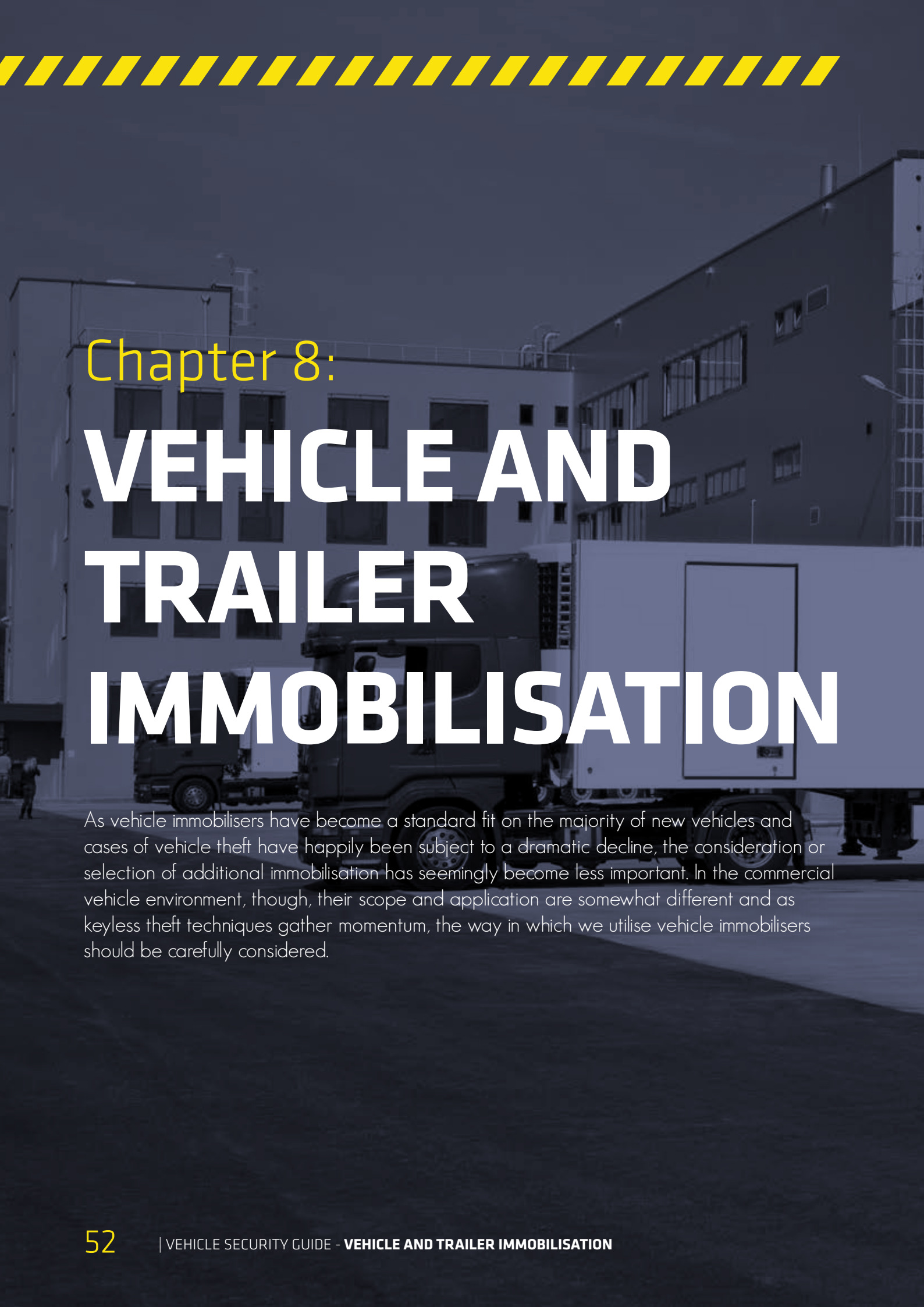
Vehicle Specification:
Think about whether or not you need glazed rear doors – they're useful for visibility, but they let everyone see what's stored in the vehicle. If possible, always opt for a solid interior bulkhead that restricts access to the load area in the event that perpetrators gain entry to the cab area.

Advertising Your Goods:
Consider whether you should be branding your vehicle. Is it necessary and important to your operations to advertise what you may be carrying or giving clues as to what value may be in the load area? If the potential risk outweighs reward, consider keeping a van as plain as possible.

Park Securely and Defensively:
Put simple procedures in place for all drivers to follow to deter criminals. If drivers take vehicles home, ensure that they are always parked in as safe and secure a location as possible, avoiding quiet or isolated areas. If conditions allow, block access to load area doors by parking against walls or other vehicles – avoid dimly lit or secluded areas and ensure that vehicles are monitored by CCTV where available.

No Valuables Stored in this Vehicle Overnight:
Wherever possible, remove valuable items overnight. If this is not feasible, consider high-quality locks for load doors and lockable toolboxes inside for valuable equipment. We've all seen the display stickers stating that no tools be left in the vehicle overnight. They're used for a reason. Any deterrent, no matter how inconsequential it may seem, is better than no deterrent.

Spare Wheels, Batteries and Cats:
Don't forget to protect exposed or easily accessible equipment that could be attractive to thieves. Loss of such items could greatly impact upon your day-to-day operations.



Chapter 8:

VEHICLE AND TRAILER IMMOBILISATION

As vehicle immobilisers have become a standard fit on the majority of new vehicles and cases of vehicle theft have happily been subject to a dramatic decline, the consideration or selection of additional immobilisation has seemingly become less important. In the commercial vehicle environment, though, their scope and application are somewhat different and as keyless theft techniques gather momentum, the way in which we utilise vehicle immobilisers should be carefully considered.

Combatting vehicle theft

The role of immobilisers has been instrumental in driving down the theft of vehicles. The 'Vehicle Crime Survey' revealed that theft of vehicles peaked in 1993, when documented cases hit almost 600,000 per annum. At this time it was estimated that only 5% of vehicles had electronic immobilisers fitted.

The theft of motor vehicles declined rapidly after this peak, partly attributed to legislative changes that made it mandatory for immobilisers to be fitted on new cars, but this was not introduced until 1998 (the UK and Germany). The widespread use of mechanical devices and interlocks was also instrumental in helping to reduce the alarmingly high rates of vehicle theft, especially on older vehicles that were not fitted with electronic, passive immobilisers as standard.

It is important to note that data refers to domestic vehicles and do not include cases of commercial vehicle theft; however, they are indicative of the changing landscape since the early 1990s. So what role does the immobiliser play today in commercial vehicles? Moreover, what can be done to protect assets where electronic immobilisers are not present (such as trailers)?

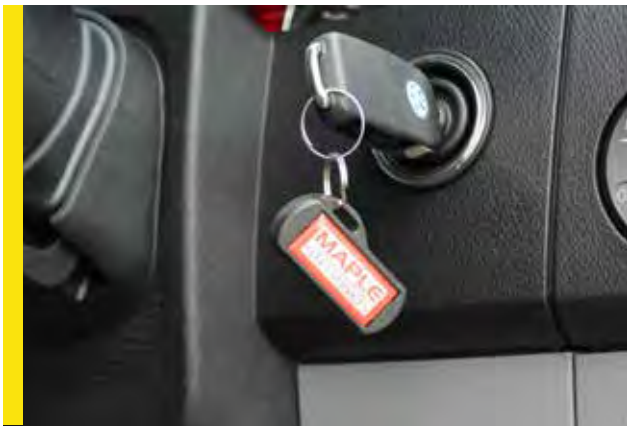
The widespread adoption of electronic immobilisers has been instrumental in driving down vehicle theft rates

Immobilisers & driver recognition solutions

Electronic immobilisers are now a standard security feature on new vehicles. They are usually passive setting systems that will isolate at least two operating systems or circuits on the vehicle. It is common practice to wire the ignition through the alarm; thus, if the alarm is triggered the vehicle is immobilised.

There are a plethora of manufacturers and aftermarket alarm/immobiliser options available on the market. In the UK it is common practice, for insurance purposes, especially for LCVs, for a certain level of Thatcham security to be attained.

As discussed in Chapter 7, the growing trend in keyless theft techniques, where thieves are able to bypass manufacturers' central locking and immobilisers, means that a secondary (after-market) immobiliser can offer a heightened level of protection against these new techniques. Operated from a separate transponder or key fob, the secondary immobiliser will stand firm in the event that the original manufacturer keys are copied or cloned.



PROTECTING IDLING VEHICLES (UNATTENDED VEHICLES WITH ENGINE RUNNING)

The thought of drivers leaving their engine running (with keys in the ignition) whilst away from the vehicle is enough to send a shiver down any transport manager's back. The meter is most definitely running as the liquid gold in the tank runs down (not to mention the fact that the driver may be committing an offence); of even greater concern, of course, is the threat of that vehicle and its contents being stolen.

A large proportion of commercial vehicle fleets are now fitted with at least one form of tracking or telematics interface. Utilising fleet management reports, instances of idling vehicles can be instantly reported, providing managers with the tools to better educate their drivers and ensure compliance.

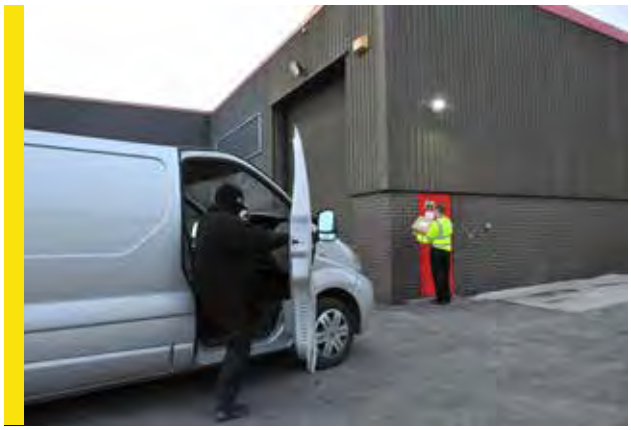
However, for certain operations, drivers may be required to leave an engine running in order to power ancillary equipment (e.g. maintenance work or bin collections), thus leaving a vehicle defenceless and exposed to theft or unauthorised movement.

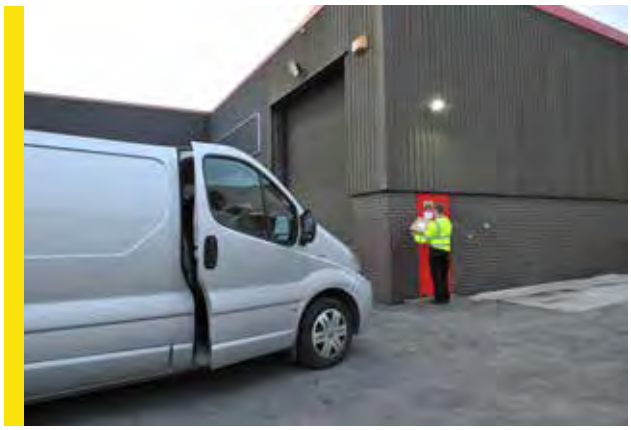
IGNITON KEYOUT & DRIVER RECOGNITION SYSTEM

Ignition Keyout systems offer an effective security measure for vehicles in which there is a requirement to keep the engine running. To initiate, the driver simply presses a dash-mounted button to remove the key. If any person attempts to move the vehicle without the ignition key present, the engine will immediately cut (usually triggered by the release of a handbrake or depressing of the clutch).

They are best suited to scenarios where a driver may be away from the cab for a prolonged period of time, usually when carrying out other work-related tasks, as opposed to multi-drop operations, where there may be a temptation or opportunity for the driver to forget to initiate the security system.

For operators requiring a greater level of security, driver recognition systems provide the perfect solution. Offering passive control, such applications will automatically set when a driver leaves the cab. Subsequent operation or movement of the vehicle will only be enabled for recognised drivers, similar to the ignition keyout. In the event of attempted unauthorised movement, the engine will instantly immobilise.





Trailer immobilisation

KINGPIN LOCKS

When considering the security of a trailer, it is primarily led by the protection of goods and preventing access to the load area, but consideration should also be given to that of the trailer itself.

The aim of immobilisation is to render a vehicle or trailer immovable and, therefore, incapable of being driven or towed away. For all of the advances in vehicle security, the most common method of immobilising a trailer is with the application of mechanical locking applications such as landing leg locks or more commonly, kingpin locks. These locks fit securely over or around the kingpin itself; once engaged it prevents a tractor unit from engaging its fifth wheel coupling with the trailer.

Fitting of a kingpin lock is, of course, a manual process. The area around the trailer's kingpin is a dirty and greasy environment, making its application an unwelcome task for the driver and perhaps contributing to such devices being underutilised and their application often being 'forgotten'.

TRAILER PARKBRAKE SECURITY

Another method of immobilising a trailer is to prevent the release of the trailer brakes via unauthorised persons.

A simple way to achieve this is with the use of an 'Airline Lock' or 'Red Line Lock' which is temporarily fitted to the airline connector on the trailer; whilst in position it prohibits illicit movement of the trailer by preventing the release of the trailers parkbrake. It should however be noted, that this is a low level security solution that could potentially be removed by force, they are perhaps better utilised for VOR trailers to prevent inadvertent movement. Furthermore, UK airline connectors are very different to common European Palm couplings, so compatability is limited.

A newer breed of trailer parkbrake security builds upon the 'driver recognition' theme, whereby drivers of connecting tractor units are unable to release trailer brakes unless authorised to do so. Integrated with trailer-coupling safety devices, they ensure that trailer brakes remain locked on until they have shown a correctly coded key fob; in doing so, they will then be able to continue their normal coupling procedure and are permitted to move the trailer - if linked with a telematics system, trailer movements could even be managed remotely.

A further advantage of modern trailer immobilisation methods, is the ability to securely tether a trailer to the tractor unit, this can be particularly advantageous in combatting hi-jack situations where a thief may remove the original tractor unit and replace with his own vehicle. Such systems operate rather like bluetooth devices, whereby you need to pair the devices before they will communicate together, once paired they will continue to operate until such time the devices are disconnected.

FAQs

Q **Is it safe and legal for my driver to go underneath a trailer to fit a king pin lock?**

A There is no specific legislation regarding the act of employees accessing the underside of the vehicle; however, in common with any other potential health and safety issue, employers should conduct a full risk assessment. In identifying any tasks or situations that could cause harm, you must determine whether you are taking reasonable steps to prevent that harm from occurring. For further information, visit the HSE website: www.hse.gov.uk/risk/.

Q **If I need to leave my vehicle running to power auxiliary equipment, how can I make it secure?**

A Under the Road Vehicles (Construction and Use) Regulations Act, unattended vehicles are not permitted to be left running unless they are engaged in activity that requires the engine to drive other equipment AND the vehicle is left in such a position and condition so as not to be likely to endanger any person or property.

Keyout applications allow the continued safe operation of the vehicle engine whilst the keys can be removed. In the event that an unauthorised attempt is made to move the vehicle, the engine will instantly immobilise. Driver recognition systems offer an additional level of protection by offering passive operation and ensuring that the vehicle is protected whenever the driver is away from the cab (regardless of whether keys have been removed or not).

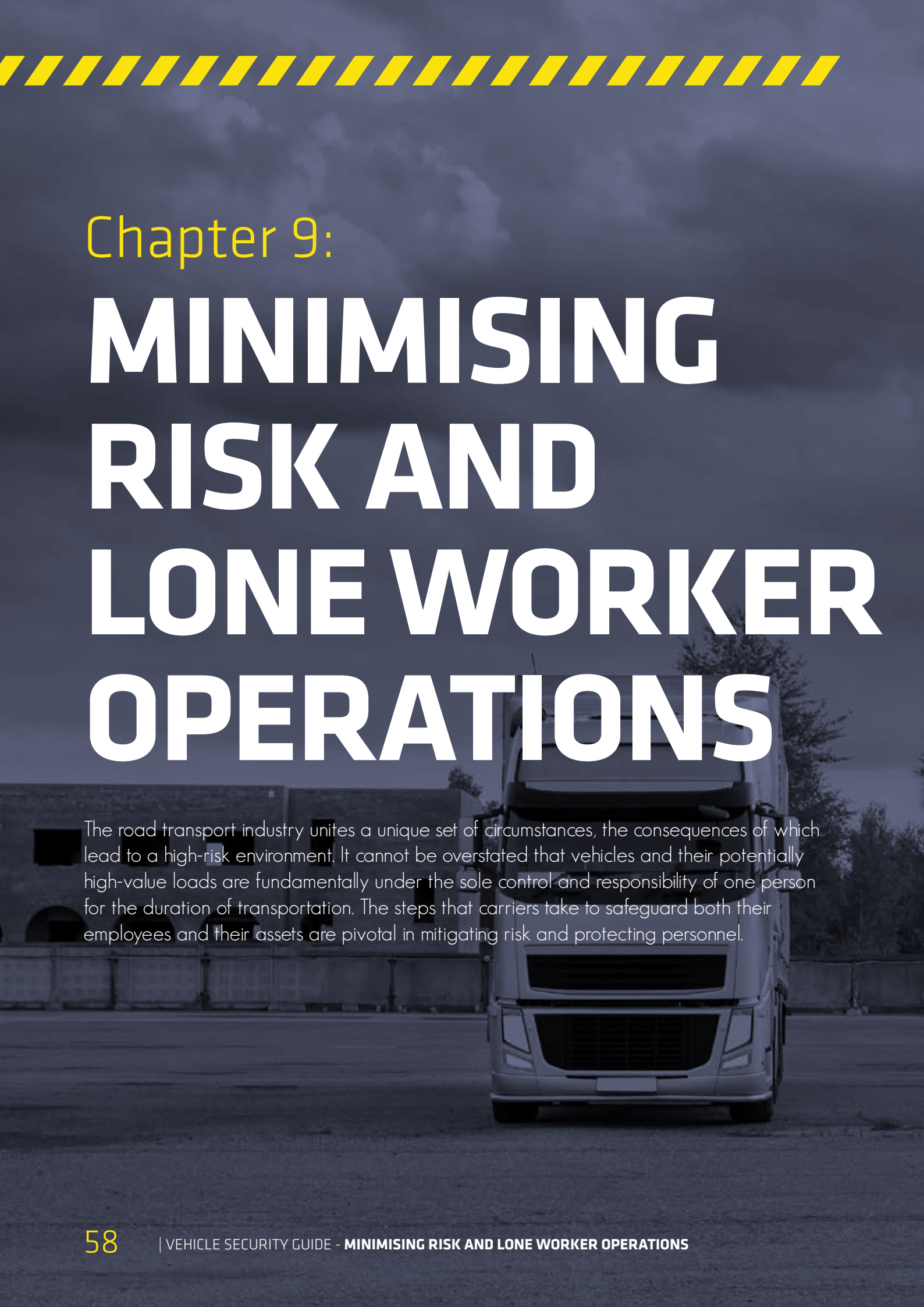
ROOF MARKINGS

Roof markings were originally devised for use on emergency service vehicles so they could be easily identified from the air. Their use is designed to assist in identifying a specific vehicle, vehicle type and/or agency.

In consultation with ACPO - Association of Chief Police Officers (now operating as NPCC - National Police Chiefs Council) and the working group JAGOLT (Joint Action Group on Lorry Theft), it was recognised that the increased use of air support by the police service provided an additional opportunity for identifying HGV's whenever this need may arise (i.e theft of vehicle, hijack situation or potential terrorist activity).

- Colour: It is recommended that only two colours are used for roof markings. Black text for use on white or lightly coloured vehicles or white text on dark coloured vehicles.
- Dimensions: This is particularly important to ensure optimum visibility at normal altitude (approximately 1000ft), thus the recommended character sizing is 300m x 300mm.
- Construction: It is also recommended that each character is constructed from reflective base material with a 15mm border of black or white matt material to the exterior and interior of each individual character.

A guide for roof markings was originally published by the 'Police Scientific Development Branch (PSDB).' To request a copy of the document (publication 14/99) contact 'The Centre for Applied Science and Technology, (CAST)' which subsequently replaced the PSDB.



Chapter 9:

MINIMISING RISK AND LONE WORKER OPERATIONS

The road transport industry unites a unique set of circumstances, the consequences of which lead to a high-risk environment. It cannot be overstated that vehicles and their potentially high-value loads are fundamentally under the sole control and responsibility of one person for the duration of transportation. The steps that carriers take to safeguard both their employees and their assets are pivotal in mitigating risk and protecting personnel.

Business resilience – self assessment

To assist in reviewing your existing systems, processes and their effectiveness in preventing commercial vehicle crime, the following information and guidance can help you to understand your current position and develop your strategy further:

It is important to review exactly where you are with regard to security and mitigating risk. You may already have some effective security measures in place, but do these go far enough? Is there scope for improvement and/or areas of vulnerability that still exist?

Almost one in seven companies suffers a major disruption during the life of its business. Without a resilience plan in place you have less chance of maintaining continuous business operations. By planning now, you can proactively ensure your resilience against and ability to manage unexpected, disruptive events that are likely to have a significant negative impact.

The Scottish Business Resilience Centre has developed an excellent '10 Steps to Business Resilience' self-assessment tool. The online tool includes a short series of questions that are designed to prompt internal thought about risk and risk appetite. On completion you will be provided with an automated resilience report, which details the proportionate level of operational risk and suggestions for mitigation of identified risks.

The assessment can be accessed at www.10steps.co.uk. Alternatively, your insurance provider may also be able to offer a similar service as part of your standard policy.

£750,000

daily cost to UK logistics as a result of Operation Stack & associated delays in 2015

91% of Drivers

consider there to be a 'serious threat' to their safety when crossing borders

6 Million

estimated number of loan workers in the UK

TAPA security standards

TAPA (Transported Asset Protection Association) have developed a set of standards which are adopted as a benchmark for supply chain standards and sometimes listed as requirements in contracts issued by manufacturers.

TAPA have produced similar standards for both facilities and trucking, with the latter (TSR, 'Trucking Security Requirements') covering the following areas. Carriers can be classified into three different TSR levels, with TSR 1 being the highest attainable.

- Management Support & Responsibilities Protocols
- Vetting & Termination of Employees Protocols
- Training
- Tracking & Tracing Protocols
- On Route Protocols
- Physical Security Requirements
- Tracking Technology
- Security Procedures
- Freight Handover Process

For more information on TAPA and becoming a member, visit www.tapaemea.com.

CyberCrime

THE TANGLED WEB

In common with most industry sectors, the internet has had a huge impact on the supply chain industries and the way in which business is conducted.

The evolution of e-commerce continues to create new opportunities and challenges in equal measure. Consumers insatiable appetite for their goods to be delivered almost instantaneously has now reached the point where items can be ordered and delivered on the same day, often within just a few short hours. These logistical challenges are intensified further by inner city restrictions on which vehicles can be used and when, creating a complex conundrum, one to which businesses are finding an impressive array of inventive solutions to.

On the other hand, the internet revolution has also provided opportunity with new platforms for doing business, in the form of online haulage exchange sites. Whilst these developments provide tantalising opportunities and access to previously unobtainable trade, users should also be wary of the potential risks they present. Criminal intent looms large on such portals, as offenders can easily create fake accounts, masquerading as seemingly legitimate hauliers with the aim of winning work to acquire goods fraudulently (for more detail see Chapter 14 which covers deception techniques).

These fraudulent techniques may be specific to the supply chain industry but there are many more cyber threats which are common to all businesses, regardless of the industry in which they operate. It is more important than ever to take a proactive approach to managing these risks and protecting business.

CURRENT & EMERGING THREATS

The way in which we use the internet evolves and expands at a phenomenal rate. So it is of little surprise that the techniques used by cyber criminals is also ever changing, not to mention impressively sophisticated. The so called 'dark web' provides the platform for criminals to obtain the latest malicious software and share advice and information on how to carry out attacks; All for relatively little cost and away from prying eyes.

One of the most ominous threats posed to business today and one which is growing in notoriety is that of ransomware. Ransomware is computer malware that installs covertly on a victim's device (e.g., computer or smartphone,) it then mounts a cryptoviral extortion attack that holds the victim's data hostage, or threatens to publish the victim's data, until a ransom is paid.

Ransomware is currently regarded as the most dangerous cyber-attack technique. One particularly 'successful' Trojan based scam known as 'CryptoWall' is estimated by the US Federal Bureau of Investigation to have accrued more than $18million in illicit earnings.

CYBER ESSENTIALS

For many companies IT security will be an integral part of their day to day business, whether it be managed internally or sub contracted to a specialist 3rd party. For others it may seem hugely daunting. Fortunately there is a great deal of advice available to ensure that you are doing the basics correctly and not leaving yourselves open to attack; the following resources can help you to keep your business safe online;

The National Cyber Security Centre (NCSC)
The UK Government's flagship cyber security agency. Their purpose is to reduce the cyber security risk to the UK by improving its cyber security and cyber resilience
www.ncsc.gov.uk

Cyber Essentials
Government and industry-backed standard which protects your business against cyber threats
www.cyberaware.gov.uk/cyberessentials

ActionFraud
In the event that you fall victim to cyber crime or fraud – incidents can be reported directly to the UK's specific reporting centre.
www.actionfraud.police.uk
(in Scotland official advice is to report to the police by calling 101).

Lone worker enviroment

According to members of the British Security Industry Association's (BSIA) Lone Worker section, professional drivers are the group facing the highest levels of risk (including those working in long-distance HGV road haulage as well as LGV or local delivery drivers).

LEGAL OBLIGATIONS

Employers should seek independent advice when drawing up protocols and procedures for the protection of lone workers, but as a minimum you should be aware of your legal obligations to keep lone workers safe, including the following:

- By law, employers are responsible for the health, safety and welfare at work of all of their employees, which also includes contractors and self-employed persons.
- Understand legal responsibilities as an employer.
- Ensure that a risk assessment is carried out and strategies implemented to provide a safe working environment for lone workers.
- Ensure that the lone worker has the relevant resources, training and information to work on their own safely.
- Have procedures in place to deal with a lone worker having an accident or signalling an emergency.

DUTY OF CARE

Your duty of care must include the following:

- Involve workers when considering potential risks and measures to control them.
- Take steps to ensure that risks are removed where possible, or put in place control measures, e.g. carefully selecting work equipment, to ensure that the worker is able to perform the required tasks in safety.
- Instruction, training and supervision.
- Reviewing risk assessments periodically or when there has been a significant change in working practice.
- Consider providing emergency may day alarms, which can be used to inform a monitoring station as to the whereabouts of the person and the fact that they may be in need of urgent assistance.

It is also important to remember that your duty of care may also extend to sub-contractors or self-employed drivers, particularly if they drive exclusively (or predominantly) for just one carrier.

For further guidance and to ensure that you are fulfilling your legal obligations with regard to lone workers, see www.hse.gov.uk/toolbox/workers/lone.htm

BS 8484:2016 PROVISION OF LONE WORKER SERVICES - CODE OF PRACTICE

BS 8484:2016 provides employers of loan workers with guidance, advice, recommendations and a benchmark when seeking a solution to reduce and/or eliminate the risk to staff operating in a lone worker environment. It is applicable to lone worker devices and lone worker applications; acknowledging that these are part of an overall lone worker protection strategy.

Providing potentially vulnerable employees with a facility to raise an alarm or call for help if they feel threatened is an important consideration for employers, helping to fulfil their duty of care responsibilities. When specifying lone worker devices/applications, it is important to note that British Standard BS8484 forms the basis for police response to lone worker systems, that are connected to an alarm receiving centre or emergency response system; thus a police response cannot be guaranteed by a supplier who isn't audited and certified to BS8484.

For further information on lone worker obligations and best practice visit www.bsia.co.uk and for more information on British Standard BS8484 visit www.bsigroup.com.

Social media supply chain risk

NEWS JUST IN...SOCIAL MEDIA UPDATES COULD PUT CARGO AT RISK

The use of social media has exploded, it is estimated more than half the population of Western Europe will be using social networks by 2019. By using such sites, users willingly relinquish personal details with little thought of the wider implications or consequences. On the face of it, the information we share may seem innocuous enough, but in the wrong hands it can quickly provide criminals with powerful intelligence; It is information that could put your cargo at risk.

WHAT INFORMATION CAN CARGO CRIMINALS USE?

Criminals can learn a great deal from social media accounts very easily. A profile may contain information about a persons employment and what their role entails. Professional platforms such as Linkedin may provide further insight into the nature of personal relationships and projects individuals are involved with, all of which help criminals to quickly build a profile of potential targets.

HOW CAN INFORMATION FROM SOCIAL MEDIA POSTS BE USED?

Whilst it is unlikely that a driver would post details about their latest consignment, with a postcode of where they are parking up overnight, they may be inclined to share a seemingly innocent update about their day or picture of their strange or stunning location, which in turn reveals just enough information about their whereabouts.

Very quickly, cargo criminals may glean who a person works for, could make an educated guess about the goods being carried and identify the approximate location of a vehicle. Furthermore, many social media sites and other mobile applications use location services. Thus that seemingly innocent update could now reveal a persons exact location, or in more sinister cases, accounts could even be hacked to track an individuals movements.

WHAT MEASURES CAN BE TAKEN?

In the age of widespread social media use, we should all exercise caution and question the information that we willingly share. Simple steps such as only accepting requests from people you know and actively tweaking security settings on individual accounts are prudent steps. From an employer's point of view within the supply chain, it is important to implement a social media policy and educate employees about good practice, ensuring they use such platforms in a responsible manner that does not jeopardise the security of the goods being carried or the safety of individuals.

Chapter 10:

DRIVER AND EMPLOYEE VETTING

There are few professions where individual members of staff are entrusted with sole responsibility for millions of pounds of goods and assets. There are fewer still where those same employees are afforded such accountability on day one, which is often the case for drivers of large goods vehicles. At least, where such anomalies of employment do occur, strict security procedures are in place. Or are they?

The importance of driver vetting

When sending your children to school you would expect that teachers be subject to DBS checks (Disclosure and Barring Service, previously Criminal Background Checks) before they are allowed anywhere near a classroom. You may assume that your GP has sufficient medical qualifications and that suitable background checks have been conducted before they are able to practice. You may also consider how bank clerks are subject to strict security checks; they are, after all, handling large amounts of cash on a daily basis.

These are all reasonable assumptions to which we expect to have been adhered by persons who hold highly responsible positions. Commercial vehicle drivers also hold a position of huge responsibility. They are in control of a large goods vehicle that has the potential to cause serious injury and even fatalities if not driven proficiently, hence the driver's CPC (Certificate of Professional Competence).

By contrast and rather absurdly, there is no legal requirement for drivers to complete security modules as part of their CPC, yet it is common practice for drivers to haul dangerous, sensitive or hugely valuable loads on a daily basis. Therefore, whilst a licence can demonstrate competency, it does not indicate suitability. The onus is very much on individual stakeholders to protect their supply chain and the integrity of the services provided; failure to get this right at the recruitment stage could lead to far more serious consequences further down the line.

It's estimated that at least 85% of cargo theft losses involve individuals with inside information. This could include the driver, warehouse staff, schedulers, etc. Your employees can relay information to accomplices about commodities, departure times, routes, destinations, and more.

Is your recruitment policy fit for purpose? Are you protecting yourselves, your clients and your business?

Employee theft & collusion

DRIVER COLLUSION

A lorry driver, working for a distribution company, was arrested for his part in the theft of a trailer and its entire load of 15,200 mobile phones, which were worth more than £1.6 million.

The theft was a well-orchestrated 'inside job' which relied heavily upon the actions and information provided by the driver, who is believed to have accepted payments of £75,000 for his part in the theft.

On the day of the alleged crime, the driver was scheduled to deliver the consignment of mobile phones to a retailer's warehouse. He is said to have informed his accomplices of the planned delivery, who met him at a lay-by. The trailer was subsequently unhooked and driven away by a second tractor unit to be unloaded.

The perpetrators then conspired to give the impression that the driver had been hijacked. He and his tractor unit were driven to a junction near the M6 motorway, where his hands and feet were tied together with cable ties. Eventually, he left the cab and drew the attention of a lorry driver parked nearby to raise the alarm.

The driver maintained throughout the trial that he was the victim of a genuine robbery, claiming that a car had collided with his lorry and he was then attacked by two Eastern European men, with Polish accents, who tied him up. The driver and two accomplices, who had met through their driving work for a courier firm used by the distribution company, were convicted for their parts in the staged robbery.

DRIVER THEFT

A delivery driver was jailed for 18 months after confessing to the theft of meat, fish and cheese to the value of nearly £50,000.

In three separate incidents the driver took vast quantities of fish worth approximately £13,000, followed by £6,000 of chicken drumsticks a month later. A few weeks later he is believed to have taken a consignment of cheese valued at close to £29,000.

The court heard that on each occasion the driver stole items while transporting goods to and from businesses and freight terminals. The discrepancies only came to light after substantial quantities were eventually identified and subsequently queried. The thefts formed part of a three-year investigation and the goods have never been recovered, resulting in substantial losses for those involved. It is not known if these were the only incidents that occurred or if other thefts went unnoticed.

The threat from within: Inside information is a valuable commodity for cargo criminals

Drivers are entrusted with high value loads, often with unrestricted access

FAQs

Q **Am I allowed to carry out security checks on people whom I employ? Do I have to ask their permission?**

A You must ask permission from applicants before carrying out a DBS check (Disclosure and Barring Service). Most jobs are covered by the Rehabilitation of Offenders Act 1974; therefore, applicants are only legally required to declare, and the employer is only entitled to know about, unspent cautions or convictions. If the applicant has been charged with an offence, an employer may be entitled to know about pending prosecutions.

Applicants should be informed from the outset about exactly what information will be requested from them and why, and at which stage of the application this information will be requested. Details about criminal records should only be requested from applicants who are offered a position of employment. This information should be obtained separately and confidentially, in the form of a disclosure statement, not as part of the application form.

For more information refer to www.acas.org.uk/index.aspx?articleid=4845 or NACRO's 'Recruiting safely and fairly' guide (www.nacro.org.uk).

Q **Can I carry out security checks on people whom I do not directly employ?**

A If it is a requirement of the position and is part of your company's own recruitment policy (see above), you are able to request that drivers provide a DBS check.

Q **Who officially carries out security checks on staff? Do I have a choice?**

A Employers can obtain background checks from the Disclosure and Barring Service, Disclosure Scotland (this service is not restricted to Scotland) or an umbrella body (a registered body that provides access to DBS checks).

Disclosure and Barring Service: www.gov.uk/disclosure-barring-service-check

Disclosure Scotland: www.disclosurescotland.co.uk

Q **What is the best way in which to check that a driving licence is genuine and up to date?**

A You can check someone's driving licence information online, including details such as the vehicles they can drive, any penalty points or disqualifications. It's free to check and available 24 hours a day: www.gov.uk/check-driving-information. Alternatively, you can also confirm licence details via phone, fax or post (see the above link). Employers should also ensure that drivers provide evidence of an up-to-date driver CPC.

Q **If I suspect one of my drivers to be committing theft, can I have an investigator follow him? Am I able to use this information in a court of law?**

A In the event that you suspect a driver to be committing theft and are able to demonstrate a reasonable basis for doing so, then monitoring or investigating your employees is perfectly lawful.

You should be mindful of complying with your own company policies and procedures and that you are acting within the boundaries of the 'Human Rights Act' (which, if followed correctly, should assist you in any investigation), but, in essence, if what you are doing is deemed reasonable for the circumstances then you may investigate.

NB: The above is applicable to the UK. Refer to your own country's specific legislation for clarity.

Vetting new employees in the supply chain

Interview Stage:
Ask the applicant to bring relevant licences and/or vocational qualifications/training. You should insist that the applicant bring the originals of all of the above documents to the interview and not photocopies.

Take Copies:
On offer of employment, request to see copies of all relevant documents, e.g. passport, driving licence, work permit (if applicable), etc., take photocopies and ensure that they are marked to confirm certification of the original. You must destroy all copies for any candidates who subsequently do not begin working for you.

Check For Consistency:
Check that all documents produced, e.g. passport, HGV licence, etc., have not passed expiry dates, that photographs and dates of birth are consistent with the applicant's appearance, and that, for foreign nationals, the documents issued allow them to undertake the job for which you are interviewing them.

Suitability:
Check that the applicant's driving licence shows the correct driving categories for the job.

Question Inconsistencies:
Any discrepancies or inconsistencies in the application form or supporting documentation provided must be queried and satisfactorily resolved. Question any gaps in the applicant's employment history and ensure that satisfactory explanations are provided for such gaps.

Pre-Employment Checks:
Inform successful applicants in writing that they are being formally offered the position advertised, subject to the immediate receipt of two years' worth of satisfactory references, a criminal record check, and undertaking necessary health checks.

Criminal Record Checks:
For British nationals this should be in the form of a Basic Disclosure Certificate. The employee obtains this certificate via Disclosure Scotland, which is a service providing criminal history checks on individuals (wherever they are in the UK, i.e. not just Scotland). Disclosure Scotland issues certificates, known as "Disclosures", which give details of an individual's criminal convictions. Please refer to the following website for full details: www.disclosurescotland.co.uk.

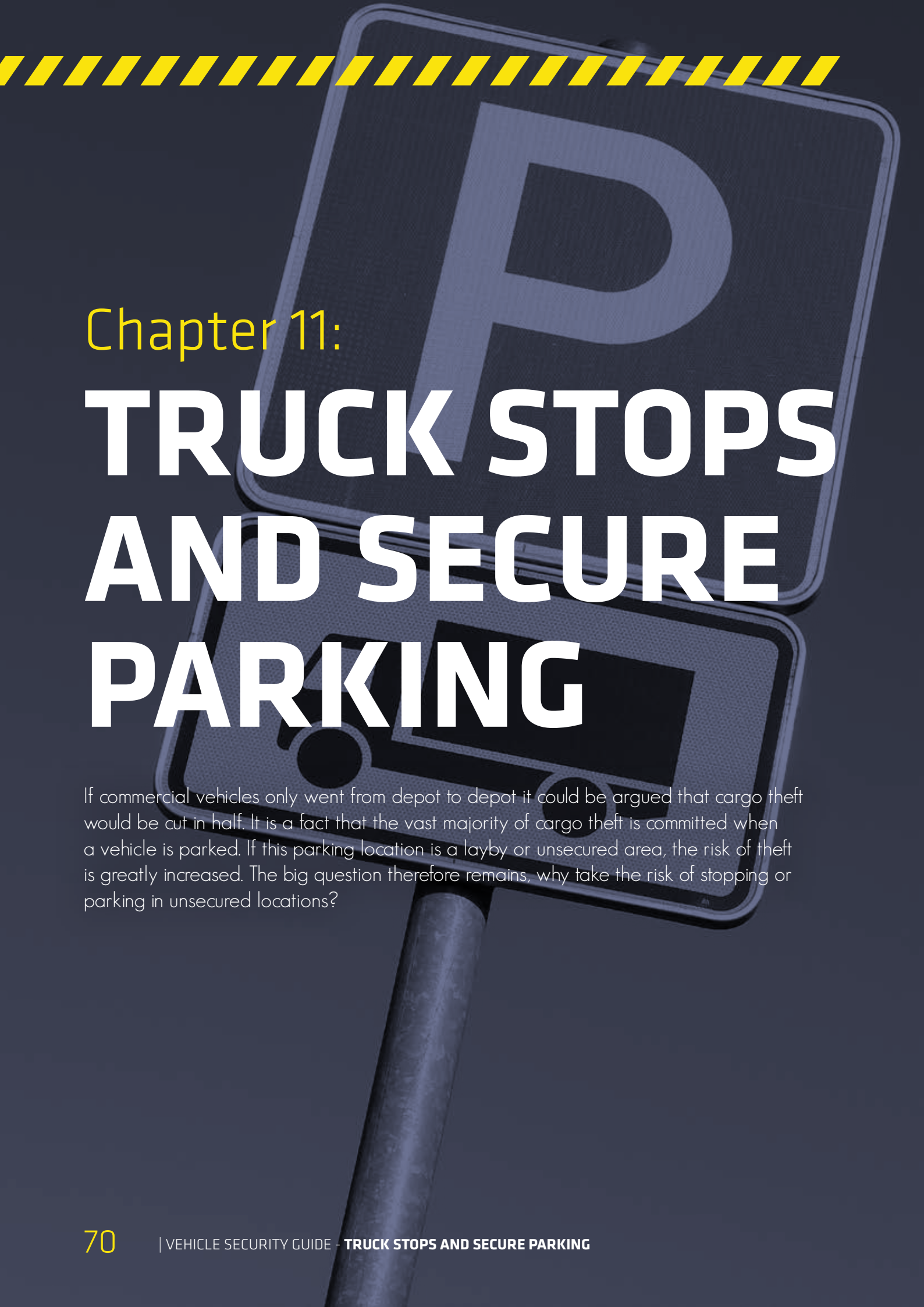
References:
Check the authenticity of all referees and employers, i.e. send requests for references or confirmation of previous employment to the registered address of the companies. If no response is received to your written requests, follow up by phone. Check the authenticity of the telephone numbers provided. If a direct line number is provided, consider contacting the main switchboard number of the business and asking for the person by name.

Timeframes:
Do not release higher-value cargo to new employees until criminal record and reference/employer checks are satisfactorily completed.

Verification:
Check licences with the DVLA, as applicants can obtain a duplicate, clean licence before the current licence is endorsed with points or disqualification.

Keep Records Up To Date:
It is recommend that six monthly appraisals be undertaken, where employees provide their original, up-to-date driving licence (if applicable) and a declaration updating:

- Driving record: accidents, offences, goods-in-transit losses, and convictions (if applicable)
- Medical history



Chapter 11:

TRUCK STOPS AND SECURE PARKING

If commercial vehicles only went from depot to depot it could be argued that cargo theft would be cut in half. It is a fact that the vast majority of cargo theft is committed when a vehicle is parked. If this parking location is a layby or unsecured area, the risk of theft is greatly increased. The big question therefore remains, why take the risk of stopping or parking in unsecured locations?

Theft from stationary vehicles

Despite the emergence of the Romanian MO (see Chapter 13), the vast majority of commercial vehicle crime occurs when a vehicle is stationary, be it when delivering goods, in the depot or parked up overnight. It is perhaps unsurprising that there is a strong correlation between vehicles parked in unsecured locations and incidents of theft, particularly cases of curtain slashing and fuel theft.

In 2016, 40.7% of cases of cargo crime were recorded in 'Unsecured Parking' areas, as opposed to 4.2% in 'Secured Parking' locations. This statistic is symbolic of the fact that across Europe there remains a dearth of adequate, secure parking locations for commercial vehicles; without private funding or government assistance it is unlikely that the number of 'secure truck parking' locations will increase dramatically. Despite calls from carriers for a greater volume of secure locations, ultimately, they are underutilised and not seen as commercially viable to operate on a large scale.

There are some initiatives which are seeking to explore the possibility of utilising alternative, existing sites for overnight truck parking, such as sports stadia, park and ride locations, and ports, but this can be hampered by suitability and the logistics of using such sites (i.e. road suitability, time restrictions, and the local environment).

Nevertheless, as with all aspects of vehicle security, there is more that carriers and drivers can do to safeguard against the threat of criminal activity and minimise risk.

The choice of parking location is one of the most important factors in security planning

Identifying secure truck parking locations

Chris Holloway, MD of Motorway Buddy (which provide a driver's smartphone app), says that parking locations can be classified into three categories: Secure, Safe and Unsafe. The Holy Grail of truck stops is that of 'secure sites'. Such locations typically feature security gates, CCTV, perimeter fencing, security guards, and good on-site facilities (showers, cafes, etc.).

Safe sites can be categorised as parking locations that cater to commercial vehicles but do not benefit from the same high-security measures adopted by the leading truck locations; motorway service stations would fall into this category, for example.

Unsafe locations are roadside parking, unofficial parking areas (e.g. industrial estates) or lay-bys. These areas are particularly vulnerable, perhaps poorly lit, and certainly uncontrolled. They are locations where you could reasonably expect to see a much higher level of criminality, as conditions lend themselves to covert activity.

When drivers and operators are deciding upon their strategy as to where to park they have a clear decision to make regarding which type of location they choose. There are contributing factors, of course, e.g. ease of access (geographically), cost of parking and who funds this (whether the driver has to pay for parking and then claim back on expenses), responsibility (i.e. whether the haulier is accountable for losses or damage or the driver is deemed responsible for the security of their vehicle), and the nature of the goods being transported. But whatever strategy is employed, the decision should be proactively made and not left to chance or whim; furthermore, it is imperative that this message be cascaded throughout the company so that the policy is clear for all parties as to what is expected and required.

Whilst drivers should always seek the guidance of their employer or traffic office with regard to official policy, they also have a responsibility of determining a secure and suitable parking location, not least for their own safety. The final decision on where exactly to park may not be left to their own discretion; ultimately, they make the final judgement. There are also occasions which might mean that a driver has to carry out unscheduled stops or is unable to reach a pre-planned rest area due to available driving hours. Both employee and employer should be clear as to what the policy is under each given circumstance.

WHERE CAN I FIND AN UP TO DATE LIST OF SECURE PARKING AREAS

There are numerous resources that claim to provide details of truck parking locations, but they can quickly become outdated (truck parks close, parking conditions/restrictions may change). IRU provides a list of European truck parking locations, together with a security rating for each site (though many of those listed are self-assessed): www.iru.org/apps/transparkapp (supported by TAPA). The Highways Agency have also produced a 'Truck Stop Guide' for locations in England but as a static guide it is not actively updated, you can download a copy from www.highways.gov.uk/publications/truckstops-in-England

Safe and secure parking

PARKING CONSIDERATIONS FOR THE HAULIER

Where to Park:
The most crucial decision concerns where you want your drivers to park overnight. You should be clear as to what is expected of your drivers and what the implications are if they deviate from this.

- Do you expect drivers to only use recognised truck stops or service stations?
- Ensure that drivers are aware of where preferred rest areas are located.
- Be clear as to whether drivers are to avoid lay-bys or unsecured areas.

Plan Ahead:
When route planning, ensure that you are making adequate considerations for parking locations, allowing enough time to reach preferred facilities. For regular destinations you may need to consider varying the routes taken to avoid being identified by criminal groups and, thus, minimise the risk of hijacking.

Reciprocal Agreements:
Consider working with other hauliers to develop mutual parking agreements at secure depots.

Load Considerations:
If you are carrying high-value or sensitive loads, take extra precautions when considering parking locations. Are there any insurance considerations for which you need to account?

Resources:
How are you going to pay for parking? Is it via an account at certain lorry parks or will drivers require cash? Parking apps allow drivers to search hundreds of parking locations across the country and pay using a built-in payment facility.

Communication/Training:
Ensure that you inform and train your drivers as to what their responsibilities are and, equally, what they need to be looking out for when making decisions on where to park.

Sub-Contractors:
Be clear in your instructions to sub-contractors and third parties about your parking policies and what is expected of them.

SELECTING A SUITABLE PARKING LOCATION – DRIVERS

Legalities:
It may seem obvious but ensure that it is legal to park in the chosen location. Are there time restraints or are you restricting access?

Identifying a Location:
Always park your vehicle in as safe and secure a location as possible, avoiding dark and secluded areas. Identify locations that may offer security fencing or have CCTV in operation. Where CCTV is present, ensure that you are within sight of the cameras.

Visual Checks:
Ask yourself if the location looks safe? Are other vehicles parked there. If not, why not? Look for graffiti or any evidence of criminal damage in the local vicinity which may indicate that it is not appropriate.

Routes:
Stick to pre-defined routes, always report diversions, and let someone know where you have parked.

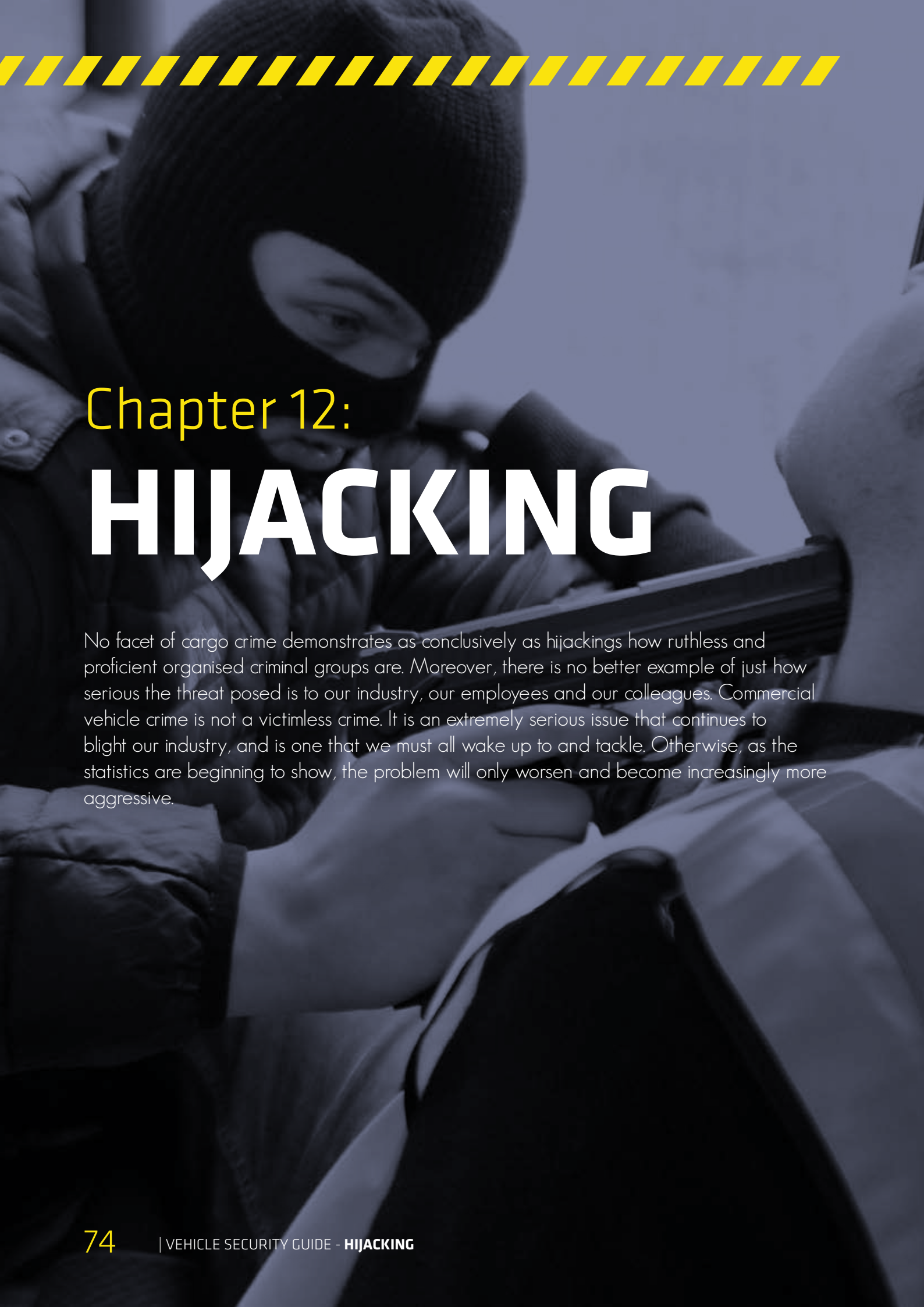
Stay Vigilant:
Be alert to threats. Watch for suspicious activity and report concerns to the police or your traffic office as soon as it is safe to do so.

Awareness:
Establish what you are carrying. Is it a high-value or vulnerable load? Secure parking locations are even more important for such consignments.

Personal Safety:
Ensure your phone is fully charged and has a signal – being able to raise the alarm in an emergency situation is vital, so take time to check.

Social Media:
Exercise caution when using social media, do not reveal what you are carrying or where you are parked, be mindful of not revealing such details to other drivers or 3rd parties

Take Precautions:
When leaving the cab, always lock the doors (it is also good practice to lock doors whilst driving) and keep your vehicle keys on you at all times. Park with the loading doors close to another vehicle or wall. When returning to your lorry, check for signs of any interference. Record your check on a checklist.



Chapter 12:
HIJACKING

No facet of cargo crime demonstrates as conclusively as hijackings how ruthless and proficient organised criminal groups are. Moreover, there is no better example of just how serious the threat posed is to our industry, our employees and our colleagues. Commercial vehicle crime is not a victimless crime. It is an extremely serious issue that continues to blight our industry, and is one that we must all wake up to and tackle. Otherwise, as the statistics are beginning to show, the problem will only worsen and become increasingly more aggressive.

Use of violence in cargo crime

Hijacking, or the taking of a vehicle by force/threat of force, is arguably the most distasteful of all cargo crime incidents. The frequency at which they occur also differs greatly, depending on location. According to official data from TAPA (Transported Asset Protection Association), such techniques are used in only 2.5% of cargo crime incidents; conversely, in some countries hijackings are far more prevalent, such as South Africa, where more than 2,000 cases were recorded in 2015 alone.

A combination of socio-economic factors, law enforcement and a high level of violent crime overall in such regions may account for the notoriety of this particular modus operandi. Yet it should also be noted that even in regions in which it is assumed that hijacking is not a major issue, there is evidence to suggest that it could be more prevalent than statistics suggest.

An article appearing in the British press, which focused on highly organised groups in the Merseyside area, cited that OCGs (Organised Criminal Gangs) had retuned their focus from cash-carrying vehicles due to the perceived high risk, and instead targeted commercial vehicles carrying high-value loads. A source claimed: "With the cash vans now, it's not worth the hassle. So you've got people who are used to making tens of thousands off a single job looking for a substitute and this is quick and easy. The serious boys do one every couple of days. They know the patterns, the routes, the lay-bys, the drivers used, everything."

Instances of hijacking in Continental Europe are generally linked to the theft or attempted theft of high-value loads. Consequently, they are well-orchestrated attacks, often utilising specialist equipment and incorporating deception techniques.

Route planning: Avoid high risk areas and vary routes to avoid being identified as a possible target by hijackers

Tactics employed by hijackers

USE OF JAMMERS

When carrying out choreographed hijack attempts, criminals will often utilise a signal jammer, which is designed to block or intercept wireless communications. Their use is widely prohibited, though it is not necessarily illegal to own such a device.

Jammers emit signals on the GPS / GPRS frequency which prevent a tracking device in the vehicle from receiving and transmitting messages, thus temporarily silencing the vehicle. Their use is intended to create a temporary veil by preventing a monitored tracking system from sending alerts about route deviation, unscheduled stops or raising any suspicion. Jammers also provide the assailants with sufficient time in which to offload the vehicle without being located.

BOGUS POLICE AND DVSA OFFICERS

In an effort to stop drivers en route, criminals have been known to impersonate police or DVSA officers (Drivers and Vehicle Standards Agency). In this scenario the impersonating officer is likely to motion for the driver to pull over and stop their vehicle immediately. Most reported instances of this nature will involve an unmarked vehicle, but there are also reports of cases where criminals will use replica vehicles.

Remain vigilant: Hijackers may attempt to impersonate officers, but are unlikely to be in marked vehicles

Highly organised criminal gangs who are experienced in undertaking such crimes may also seek to reduce the risk of being disturbed or spotted while committing the crime by closing off a small section of the road. They may set up a mock road diversion or closed-road scenario to prevent any other road users from travelling the same section of road during the planned attack.

It is important to remember that genuine officers usually stop vehicles in marked cars and they should have no objection to being asked to verify their details. If you or your drivers are asked to pull over, do so in a safe and controlled manner. Ensure that it is a well-lit, public area and telephone your employer immediately to advise them that you have been stopped (see page 84 regarding the use of vulnerable load cards). Look for signs of any anomalies in the person asking you to stop (eg. does the uniform appear genuine, are they wearing correct or appropriate footwear etc)

If you're carrying a high-value load or are suspicious of the persons asking you to stop, you can keep your engine running, doors locked and windows closed until you're sure that they are genuine. You should be mindful that in the event that you fail to stop for a genuine DVSA or police officer, you are committing an offence, which can lead to court action or even your licence being revoked.

SECURITY SOLUTIONS TO COUNTER HIJACKING

Engineered solutions designed to counter attempted hi-jack situations, generally centre around protecting the driver via early warning indicators or making the subsequent getaway as difficult as possible for the perpetrator, rather than physically preventing the initial attack itself.

TRACKING SYSTEMS

As referenced earlier, it is commonplace for jamming devices to be used in cases of hijacking. Some telematics systems are able to detect early interference of the GPS signal; in doing so, they are then able to transmit an emergency mayday message, usually via the GPRS frequency. However, their success is dependant on being able to detect the jammer early enough that the alert notification can be transmitted, before the GPRS signal is completely swamped (as well as the GPS signal) by the more powerful radio signal jamming device.

In practice the window for identifying the use of signal interference is very small, as hijackers are unlikely to activate a jamming device until they are ready to intercept a vehicle or have already done so. A jammer becomes more effective when in close proximity (to its intended target) and consequently if powerful enough is likely to also block any subsequent GPRS mayday signal.

It is feasible to reduce the impact of jammers, for example with the use of directional antennas which can be positioned in such a way so that the ability of the jammer to engulf and impede a vehicles telematics signal is significantly reduced. Alternatively the use of Iridium satellite tracking (i.e orbiting satellite systems as used by satellite-phones) can provide a more difficult signal to impede with common jammer devices than that of traditional GPS/GPRS based systems.

In short, communication and geo-positioning technology exists where any attempt to cause signal interference via the use of a jammer can be extremely difficult if not Impossible to achieve. However, such equipment is generally very expensive and subsequently their adoption is limited to military or other niche operations.

DRIVER PANIC ALARMS

It is essential that drivers are able to communicate with the back-office team, having the means to quickly and easily raise the alarm in the event that they suspect there may be suspicious activity or, indeed, if they are under attack, which is what a panic alarm is designed to do (via integration with telematics).

The most important consideration when selecting a panic alarm is whether you wish to have an alarm that can be raised discreetly without the assailant realising or if you would prefer an alarm that also has functionality in deterring hijackers and alerting others to the obvious duress. With regard to hijacking events it is prudent to bear in mind that such attacks are more likely to occur in secluded locations, where the potential for witnesses is low. The use of such alarms in this instance may therefore be unsuitable, or even counterproductive if it forces the hijackers into acting with more haste.

Lone worker alarms (or mayday alarms), which operate independent of a vehicle's tracking system and protect the driver if they are away from the vehicle, may also be worth consideration. Lone worker devices also have the capabilities of providing two-way communication, so monitoring staff are able to hear real-time audio without having to speak directly to the lone worker/driver (as with tracking systems, the use of jammers may prevent mayday alarms from functioning correctly).

Some tracking systems offers distress notifications

Panic alarms or mayday alarms allow drivers to discreetly call for help

ANTI-HIJACK SYSTEMS

Due to the usually aggressive nature and threats to a driver's personal safety, physically preventing an actual hijack event is almost impossible. However, commercial vehicle security providers, have, for many years marketed systems that are designed to gradually degrade and limit a vehicles performance, making such attempts far more difficult and a subsequent getaway more problematic.

It is assumed that in the event of a hijack situation the driver would be unable and/or perhaps unwilling (do not wish to draw attention to any non-compliance with the hijackers) to raise the alarm, thus a vehicle can be automatically placed into a 'hijack mode' by the triggering of a 'threat event,' such as a cab door being opened whilst the engine is running.

After a pre determined period of time a vehicle's performance will gradually diminish, thus maximum speed will be capped and acceleration restricted. Other triggers such as external alarms and flashing of headlights or indicators can be utilised though operators should be mindful that a driver may be in a hostage situation and attracting attention to the crime in progress may not be in the drivers best interests.

In years gone by, security providers have been known to manipulate vehicle performance to give the impression of a pending breakdown i.e fluctuating fuel flow so vehicle becomes erratic when driving and even generating smoke. As commercial vehicles have become far more reliable though, this particular tactic is now unrealistic.

The use of anti hi-jack systems are designed to try and increase the risk of perpetrators being caught in the act, without putting a driver in any greater danger so operators should give careful consideration to what features they adopt when employing the use of such systems.

Anti hijack systems degrade vehicle performance

IN-VEHICLE CCTV

Advances in camera technology and mobile data communications have enabled in-vehicle CCTV to make huge strides in recent years.

High-definition recording capabilities, ruggedised DVRs (Digital Video Recorders) and real-time video streaming over mobile networks provide operators with a plethora of additional tools in dealing with commercial vehicle crime.

Basic systems may be used for monitoring and data capture purposes only; thus, they can be used in the traditional guise of providing video evidence in the event of a suspected theft. Captured data can be reviewed by time and date stamps to view specifics of the event. Any number of cameras, covering various viewpoints, can be specified to offer as much evidence as possible when carrying out investigations.

Advanced functionality provides operators with remote monitoring and live video streaming of the CCTV system. A range of trigger events can provide notification of potential threat events, such as door openings (when the ignition is switched on), geo-fencing (i.e. route deviation alerts), an idle engine (i.e. alerting control room operators whenever a vehicle is left running in a fixed location for too long), and driver panic alarms.

Vehicle CCTV can now provide real time video streaming

FAQs

Q **Can I legally stop my vehicle from a remote control room if it is hijacked? I have also heard that there is a system that exists whereby a police car following my vehicle could remotely stop my vehicle in the event of public safety or a breach in security. Is this true?**

A Technically, it has been possible for many years to immobilise a vehicle from a remote location, but the legalities around the actual act of stopping a vehicle are somewhat of a grey area. They are also subject to a potential legislative review. The existing EU Directive (95/56/EC) currently prevents the complete immobilisation or stopping of a vehicle until such a point that the engine is stopped, though it does not prevent the limiting of a vehicle's speed/performance.

The issue has gained fresh momentum in light of recent terrorist activity, where trucks have been used in Trojan horse-style attacks. It is known that technology exists and has been trialled, whereby the police have the ability to bring a vehicle to a complete stop (via radio frequency technology), should it be determined that it is in the interests of public safety. Furthermore the existing legislation which currently prevents such practices is currently being challenged; it is therefore conceivable that the use of this technology could very soon be permissible.

With pending legislative changes it is therefore entirely plausible that enhanced security offerings from vehicle manufacturers or 3rd party suppliers, enabling operators to remotely immobilise vehicles, could soon become a reality.

Q **Is my driver required to stop for the police, or can he show them a vulnerable load card and follow them to the nearest police station?**

A Failure to stop for a genuine DVSA or police officer is an offence; thus, if you are suspicious about the identity of the officer who has stopped you, exercise caution. Official guidance is as follows:

1. Ensure that your vehicle doors are locked, stay in your cab, keep the engine running, and secure the parking brake.
2. If you're in contact with your operating centre, tell them your location and the reason why you've been stopped.
3. Ask the officer to verify whom they are by an ID warrant card. If you are carrying a vulnerable load card, show them. It states that you are under instruction not to open the vehicle until you have confirmed their ID (name, number and station).
4. Dial 101 (if you are suspicious or concerned that you may come under attack, dial 999) and tell the police what vulnerable/dangerous load you're carrying, your location, and the officer's ID. The officer will also contact the police control room to inform them that they've stopped you.
5. If it is a legitimate stop, by uniformed officers in a marked police vehicle, follow the officer's instructions.

Q **Can I put cameras and listening devices in the cab of my vehicles? What if the driver sleeps inside the vehicle? Is this legal? Do I need his permission?**

A As an employer you do have the right to monitor workers' activities, including recording on CCTV (and videoing outside of the workplace). This is covered by data protection laws, which include rules about the circumstances and the way in which monitoring should be carried out. It is important to be open and honest about why you are recording and what benefits you hope to gain from this, and to consider if directly recording your drivers will have any negative effects (impact assessment).

You should also inform drivers that they are being monitored on CCTV. Secret recording can often be illegal. Employers should also consider gaining employees' consent for surveillance. Incorporating it within employment contracts offers a simple way of doing so; ideally, an employer should have a code of conduct or policy that covers workplace monitoring.

Further consideration must also be afforded to operations in which drivers sleep in their vehicles, and any potential invasion of their privacy.

NB: The above is applicable to the UK. Refer to your own country's specific legislation for clarity.

Q **Can video and audio footage be used as evidence?**

A There are numerous examples of footage from in-cab recording cameras being used as evidence (in the UK) when involved in accidents or against cash-for-crash claims. There are no specific legislative considerations for the use of CCTV in vehicles. Employers should ensure that they are informing employees of the cameras on their vehicle (and seeking their consent, where appropriate), whilst conforming to data protection laws. You should also make provision for advising members of the public that vehicles are fitted with CCTV cameras, where appropriate.

For more information, refer to the CCTV code of practice issued by ICO (Information Commissioners Office) www.ico.org.uk/for-organisations/guide-to-data-protection/cctv/

Guarding against hijack situations

ADVICE FOR CARRIERS

Security Escorts:
Where high-risk routes or areas are being negotiated, particularly when transporting high-value loads, consider utilising security escorts.

Vehicle Security:
Guarding against hijacking is difficult, but tracking systems (route deviation) and driver panic alarms can, at least, provide early warning signs in the event of unusual or unexpected behaviour. Specific hijack solutions that can limit the performance of a vehicle post hijack can also provide protection to your assets and potentially minimise any losses.

Familiarity Breeds Contempt:
Hijackings are generally well-planned-out attacks and criminals will research targets thoroughly. They will target specific loads, knowing your regular movements and schedules. Minimise risk and seek to remain off criminals' radar by varying the routes and times for undertaking certain journeys, especially if they are in or around hotspot areas.

No-Stop Policy:
Where feasible, enforce a no-stop policy. For longer journeys or where this is not possible, identify high-risk areas, implement an exclusion zone, and only stop in pre-assigned rest areas (see the secure parking section).

Keep A Log:
Keep details of any suspicious activity reported by drivers. If you identify any trends or specific vehicles that are suspected of following your drivers, take action to avoid certain routes and report the details to the police.

ADVICE FOR DRIVERS

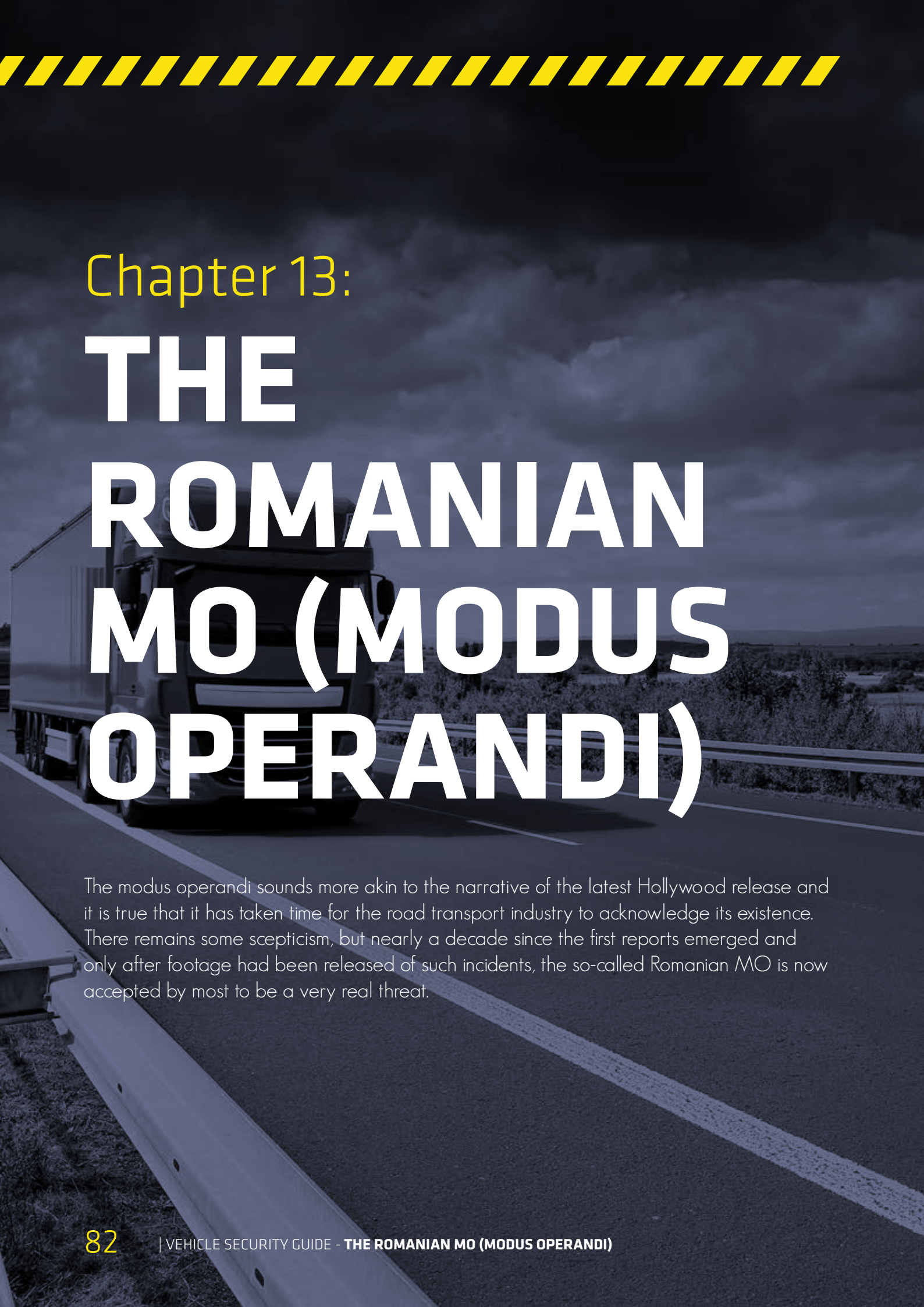
Remember the Basics:
Do not stop for hitchhikers or to help motorists in trouble; instead, call for assistance. Lock and secure your vehicle before embarking on your journey, keep windows shut, and adjust mirrors to give you the best possible view.

Mobile Phone:
Ensure that your mobile phone is fully charged before departure and keep it about your person (not on the dash or in the vehicle). You may need it!

Remain Vigilant:
Watch for suspicious vehicles or unusual activity. Are you being followed? Have you seen the same vehicle before? If you suspect anything, raise the alarm. If you suspect that you have been followed at any point, make a mental note of any details (location, vehicle make and model, etc.). If you have CCTV, note the time so that data can be reviewed later.

Exercise Caution if Stopped:
In the event that you are requested to stop by the police or DVSA, ensure that you only pull over in a safe, well-lit and public place. Telephone your manager immediately to advise them of the incident. Look for any anomalies in the person asking you to stop (eg. does the uniform appear genuine, are they wearing correct or appropriate footwear etc). DVSA officials should always be in marked cars. If you are suspicious, ask them to verify whom they are and always keep your engine running, doors locked and windows closed until you're sure that they are genuine.

In the Event of Hijack:
Do not attempt to resist. Follow instructions without resistance and do as the hijackers ask. Remember that assailants are usually armed and dangerous. Raise the alarm at the first opportunity and try to provide as much detail about your attackers and their vehicles as possible.



Chapter 13:

THE ROMANIAN MO (MODUS OPERANDI)

The modus operandi sounds more akin to the narrative of the latest Hollywood release and it is true that it has taken time for the road transport industry to acknowledge its existence. There remains some scepticism, but nearly a decade since the first reports emerged and only after footage had been released of such incidents, the so-called Romanian MO is now accepted by most to be a very real threat.

What is the Romanian MO?

The MO is believed to originate from Romania, hence the name, with the first reports cited around 2008. The tactic involves the use of specially equipped vehicles that enable criminals to closely follow a truck or trailer during transit. The perpetrator is then able to board the vehicle, usually at high speeds (to avoid detection), and offload contents to an accomplice in the following vehicle.

Unlike other forms of commercial vehicle crime, the Romanian MO is still a relatively new phenomenon. This, coupled with the seemingly implausible nature of the crime, means that it is not, as yet, being treated as a significant threat by the industry, nor are law enforcement agencies offering adequate support.

RISK VS. REWARD

OCGs (Organised Criminal Gangs) recognise the ability to access large volumes of highly sought-after goods and, to this end, they are increasingly willing to employ extreme measures to land lucrative targets. There has been for some time a very real concern that the Romanian MO may pose the most significant security threat to the movement of goods in the supply chain. A study on the 'Theft of Pharmaceuticals during Transport in Europe' revealed that transport professionals within this sector identified 'Theft from Moving Trailers' to be the trend that they classified as posing the most risk to cargo theft.

This is an extreme tactic, with reports recently emerging of the extraordinary lengths to which criminals are willing to go for rich rewards. There are cases in which access to the load area has been made via the roof, and an increasing number of attacks that involve the grinding of exterior-mounted door locks (whilst the vehicle is moving).

Reports of theft from moving vehicles are on the increase

The evolution of the Romanian MO

2008

Isolated cases in Spain and Italy in which trucks arrived with broken locks and seals but had not stopped en route – no plausible explanation. Later that year, German police arrest six Romanian men carrying out attempted theft from a moving vehicle.

JUNE 2012

Police from Romania's Department for Organised Crime and Terrorism (DIICOT) film a gang of thieves breaking into a moving truck. The footage shows two men climbing out of the sunroof. One then positions himself on the bonnet, as the other holds his legs, before breaking into the truck. The gangs were suspected of carrying out multiple attacks in a three-month period.

MAY 2014

Eleven men, of Eastern European decent, detained whilst travelling along the M6 motorway in Staffordshire on suspicion of planning to carry out theft from moving vehicles. Their vehicle had a makeshift hatch cut in the roof and a large amount of cutting equipment on board.

MARCH 2015

€100k of cigarettes stolen from a moving vehicle on the M7 motorway in Ireland. Vehicles are believed to have been travelling at speeds of up to 80KPH. Thieves used spray paint on the on-board CCTV cameras and were suspected to have been on the vehicle for up to 30 mins.

MARCH 2016

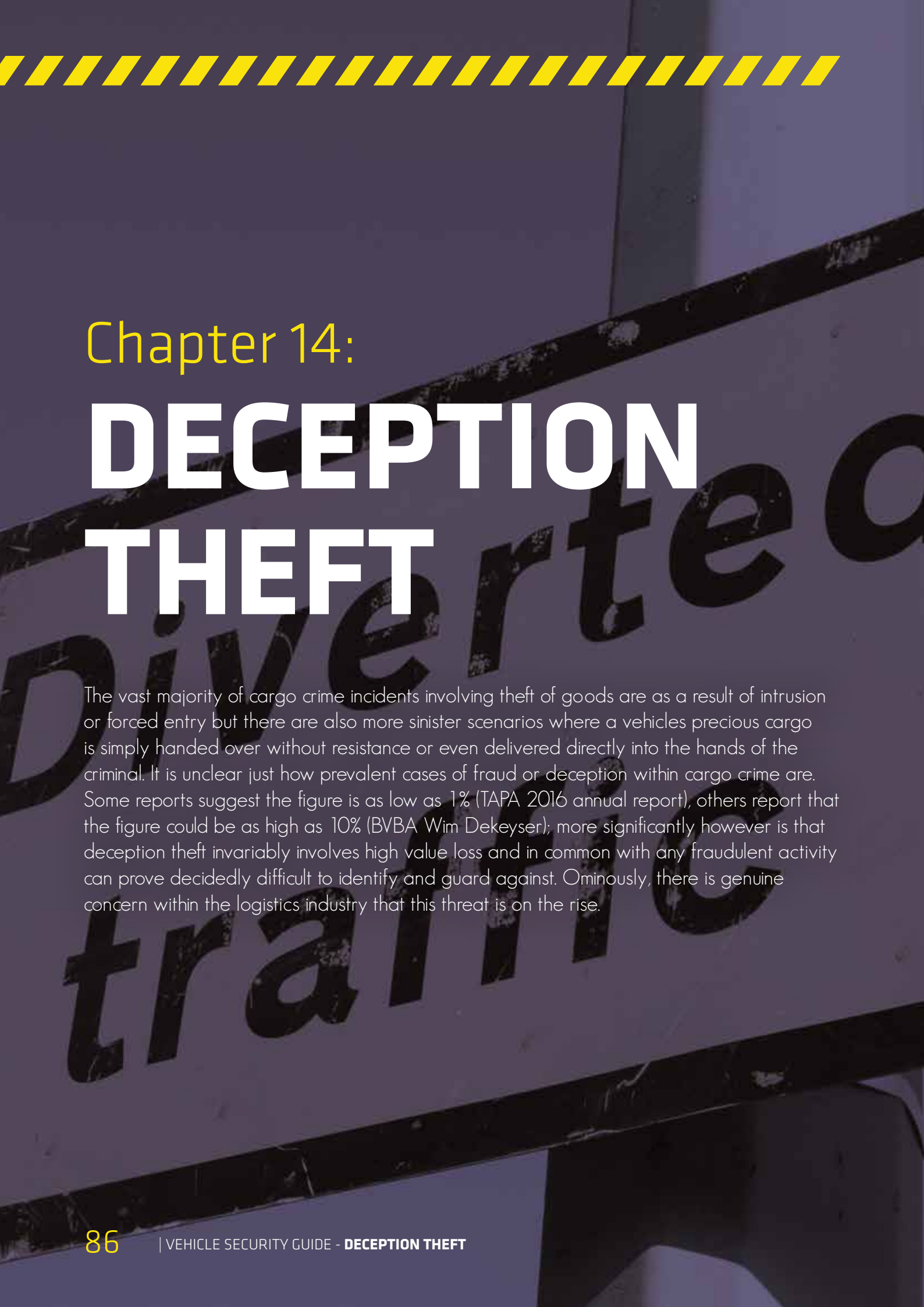
Reports in China confirm a number of incidents involving threats from moving vehicles, including the loss of $55,000 in pharmaceuticals and $40,000 in leather goods.

DOOR OPEN WARNING SYSTEMS

Given the methods employed by executors of theft from moving vehicles and the fact drivers are, in most cases, oblivious to the crime being undertaken, awareness is critical.

A simple and cost effective measure that could be adopted by vehicle operators to raise awareness of unauthorised load area breaches is a door opening warning mechanism. Standard options would alert drivers the moment a load area door is opened (when the engine is running) via an in cab LED or audible siren. In addition, a notification could be transmitted via an on-board telematics system to a remote monitoring station.

For tractor and trailer combinations, technology exists whereby drivers are able to pair a portable receiver (similar to a pager) to a trailer based transmitter, thus offering compatibility with any connecting tractor unit.



Chapter 14:

DECEPTION THEFT

The vast majority of cargo crime incidents involving theft of goods are as a result of intrusion or forced entry but there are also more sinister scenarios where a vehicles precious cargo is simply handed over without resistance or even delivered directly into the hands of the criminal. It is unclear just how prevalent cases of fraud or deception within cargo crime are. Some reports suggest the figure is as low as 1% (TAPA 2016 annual report), others report that the figure could be as high as 10% (BVBA Wim Dekeyser); more significantly however is that deception theft invariably involves high value loss and in common with any fraudulent activity can prove decidedly difficult to identify and guard against. Ominously, there is genuine concern within the logistics industry that this threat is on the rise.

Diversion & fraudulent techniques

Diversion tactics are often treated with scepticism, tales of such incidents seemingly appear to be farfetched or perhaps more cynically it is suspected collusion is afoot. In truth it can be particularly difficult to detect, diversion tactics by their very design appear to be entirely plausible and the architects of such scams are calm and resolute in their approach.

Exercise caution if asked to deviate from the original unloading instruction

ROUND THE CORNER GAME

One of the oldest tricks in the book – all be it with various interpretations, 'Round the Corner Theft' or 'Round the Corner Game' has been around since the horse and cart. It involves a perpetrator, disguised as an employee of the receiver, usually in a replica uniform or official looking attire who will divert a driver with a seemingly innocuous cover story. Typical examples may include faulty loading bay doors, long queues or flooded warehouses. The perpetrator will direct the driver to an alternative location 'round the corner' whereby they will be assisted in unloading.

Incidents of 'round the corner theft' are usually well orchestrated crimes arousing as little suspicion to a driver as possible. In one such case, where the theft of £1million worth of consumer electronics was undertaken, the driver reported 'that he found the various people concerned to be relaxed and friendly and did not appreciate at any time that he was the victim of a scam.'

BOGUS POLICE & DVSA OFFICERS

In an effort to stop drivers en route, criminals have been known to impersonate Police or DVSA (Drivers and Vehicle Standards Agency) officers. In this scenario the impersonating officer is likely to motion for the driver to pull-over and stop their vehicle immediately. Most reported instances of this nature will involve an unmarked vehicle but there are also reports of cases where criminals will use replica vehicles.

In incidents were criminals are impersonating officials, they can be of a more sinister nature and are classed as hijackings, where drivers are often subjected to physical danger. It is important to remember that genuine officers usually stop vehicles in marked cars and they should have no objection to being asked to verify their details. If you or your drivers are asked to pull-over, do so in a safe and controlled manner, ensure it is a well lit, public area and telephone your employer immediately to advise them you have been stopped.

For more information on dealing with suspicious stops see page 74 and page 78 for guidance on use of a vulnerable load card.

Fictitious collections & bogus carriers

A growing trend in deception theft is that of bogus carriers or fictitious pick-ups , accelerated by the increase in freight exchange platforms.

Fictitious pick-up is a fraudulent technique whereby criminals pose as legitimate truck drivers, sometimes even going so far as to set up fake haulage companies to do so. Criminals use online freight exchange sites to win contracts or simply show up with fake credentials (having acquired information about an assignment). The deception can be particularly difficult to identify as the collection has seemingly been legitimately arranged and consequently suspicion is naturally low when the supposed carrier arrives.

Example 1
FRAUDULENT COLLECTION

A haulier is in possession of containers of electronic goods. The principal carrier provides instructions via email to release specific containers to a subcontractor – they provide details of unique reference numbers, which in turn should be quoted by the specified subcontractor upon collection. The subcontractor is also explicitly named in the email.

The first of three vehicles arrive, they confirm which subcontractor they are representing and quote the unique reference number as alluded to in the earlier email communication. Having seemingly proven their credentials and not aroused any suspicion, the driver is allowed to leave with one of the containers. This is repeated twice more, including a second collection by the first vehicle.

The violation only came to light when containers did not arrive at the scheduled delivery point. It was subsequently discovered that the carrier was bogus and had inside information regarding the make-up of the unique references numbers.

Example 2
BOGUS CARRIER

Freight Forwarder used an on-line freight exchange portal to attract carriers for consignments of electrical goods that they needed to move from Italy to the UK.

An enquiry was made by an Italian company via telephone, with a lady who gave a name, landline and mobile number, she requested that communication was via mobile due to a problem with the landline. The email address provided appeared to be of a format that was consistent with the company name. Copies of insurance were requested and duly supplied.

Eventually an agreement was reached for the 4 trailers to be moved to the UK. The deliveries never arrived. All attempts to contact the company failed. It was later discovered that the landline telephone number was an Internet based virtual number that was no longer in use, the mobile number was suspected to be a disposable pay as you go. The Email address was a free web based domain, where the true identification of the user is difficult to trace.

The insurance policy provided was genuine, as was the actual name and details of the company but falsely supplied – the issuing insurer later confirmed that they had discovered the same policy details had been used to secure instructions in two other cases. When investigators attended the advised address of the carrier in Italy, they discovered that the firm was once a genuine company, but had ceased trading some time ago – criminals had simply used their identity to obtain insurance and pose as a bona fide carrier.

Guidance for guarding against deception theft & fraudulent activity

ADVICE FOR CARRIERS

Secure Supply Chain:
Ensure you know who is carrying your goods. Develop relationships with carriers, shippers, forwarders and consignees.

Transparency:
Know where your cargo is and who is responsible for it at all times - ensure you have visibility of real-time telematics data.

Carrier Vetting:
Know who is carrying your goods. Perform background checks, confirm email addresses, telephone numbers and websites are genuine and consistent, phone the telephone numbers for additional verification.

Driver Vetting:
Ensure you are carrying out best practice when employing new drivers (see chapter 10) If in doubt, always check and verify details until you are comfortable.

Driver Training:
Provide sufficient and relevant security training for employees and drivers, particularly for those involved with valuable cargo movements.

Clear Procedures:
Procedures for both collection and delivery of goods should be clear and well communicated, provide written instruction for carriers and drivers, making provision for audit trails.

Encourage Feedback:
Encourage feedback from staff and conduct regular audits, thus facilitating a security culture with the company. As business changes and adapts, so too security procedures should evolve.

ADVICE FOR DRIVERS

Confirm Details with your Manager:
If you are asked to deviate from the usual or scheduled delivery destination ALWAYS check with your own manager or transport officer.

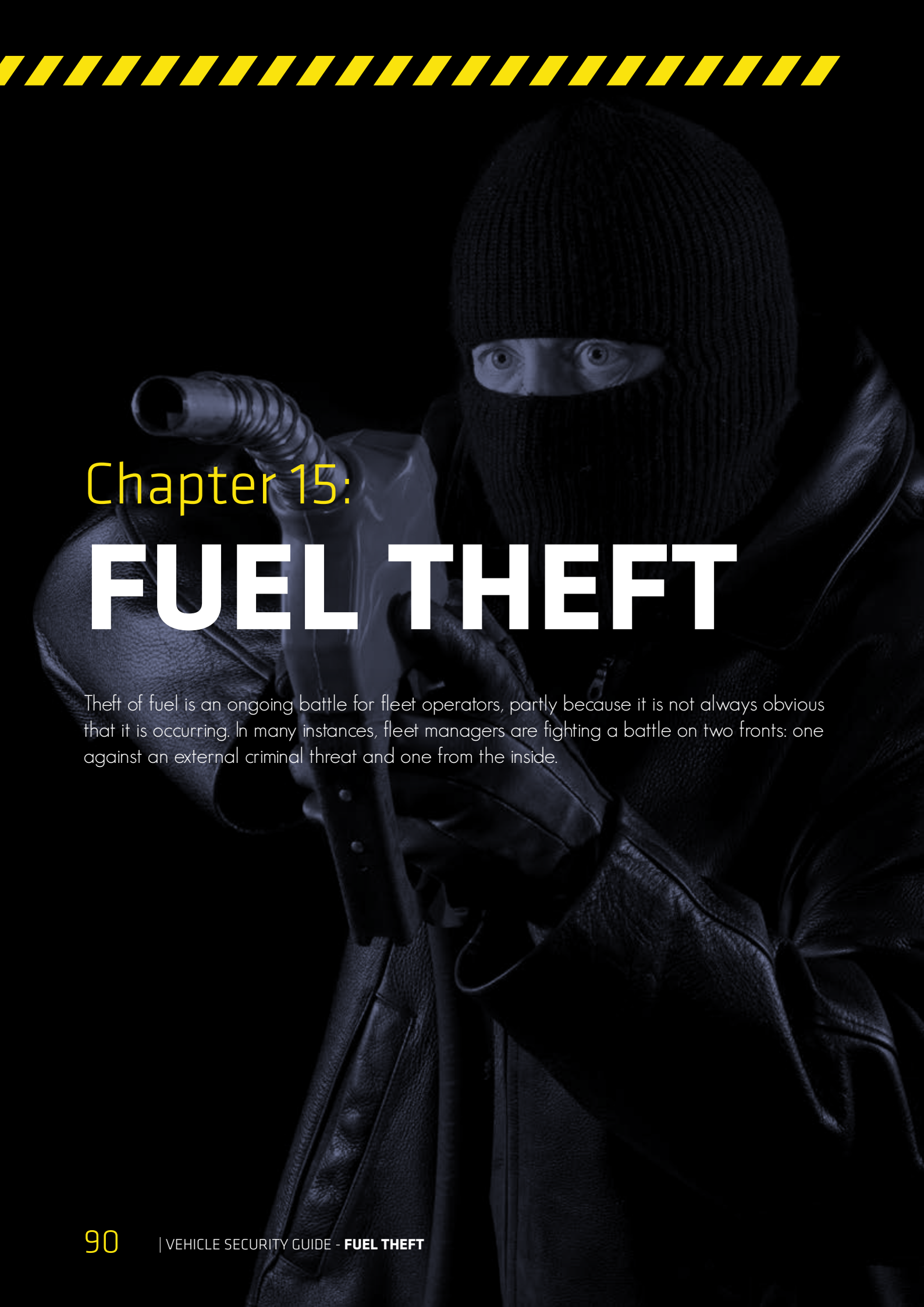
Verify Changes:
If you receive a telephone call, (particularly from an unrecognised number) asking you to divert to another destination, always verify the details with your manager or transport officer.

Written Confirmation:
If the delivery instructions do change, get written confirmation of the changes from senior staff of the original destination or from your employer

Unloading:
Never transfer the load into another vehicle instead of to the original destination, if requested to do so make sure there is a clear signature and printed name on all delivery paperwork

Visual Checks:
If you are asked to deliver to an alternative location, look for signs that the new location is associated to the original. If the new location is for sale / to let or appears to be in poor repair, proceed with caution. Also be weary of any person asking you to re-route who acts with urgency.

Check, Verify, Confirm:
If in doubt, always check and verify details until you are comfortable.



Chapter 15:
FUEL THEFT

Theft of fuel is an ongoing battle for fleet operators, partly because it is not always obvious that it is occurring. In many instances, fleet managers are fighting a battle on two fronts: one against an external criminal threat and one from the inside.

Mining for liquid gold

Fuel theft is the most prominent of all commercial vehicle crime incidents.

When UK-based TruckPol (before being disbanded) issued its last crime report in 2011 it cited the fact that, due to the huge increase in such crime, fuel theft was to be classified separately, so as not to distort the overall picture.

Unsurprisingly, there is a correlation between fuel price and fuel theft; indeed, the thefts recorded up to the aforementioned period followed a sustained period during which prices at the pump had climbed from less than £1 p/litre in 2009 to more than £1.20 p/litre in 2011.

TARGETED FUEL THEFT

Consistent with other forms of vehicle crime, fuel theft is invariably committed by specific gangs. Attacks are therefore primarily focused upon busy freight corridors that provide high volumes of traffic and opportunity. In 2015, Nottinghamshire Police launched 'Operation Magna', an initiative to increase patrols and gather intelligence on the A1, which covered a 40-mile stretch between Harworth and Newark. The operation was launched to combat a series of thefts, which included 99 reported incidents of fuel theft and 38 incidents of theft from curtain-sided trucks in just seven months; it is assumed that many more cases will have gone unreported during the same period.

The majority of incidents targeted lorries parked in rest areas and lay-bys, where thieves are believed to lie in wait in nearby farmland before accessing lorries on foot. Most thefts tend to involve the siphoning of fuel, as this method allows the thief to control the flow of fuel into a transporting vessel; rarely are the fuel tanks themselves punctured and, consequently, depending on the volume that is taken, a large number of incidents may not be detected by the driver.

Operation Magna led to a 25% reduction in the number of reported thefts and to eight arrests. However, highlighting the difficulty in detecting and even preventing the attacks themselves, despite the arrests, convictions were unsuccessful due to insufficient evidence. A lack of CCTV in dimly lit rest areas and lay-bys not only contributes to the perfect platform for illicit activity, but also makes capture inherently difficult.

INTERNAL THEFT

Perhaps even more distasteful is the issue of internal fuel theft, a seemingly widespread problem. In a survey conducted by Maple Fleet Services, 38% of respondents suspected that their own employees were responsible for fuel theft. Depending on the nature of the crime and how disciplined the offender is (i.e. siphoning small amounts of fuel but on numerous occasions), detection can be difficult.

For commercial transport companies, who consume vast amounts of fuel, the opportunity for employees to steal fuel for their own personal use is both alluring and seemingly low-risk. Typically, employees may, during the refuelling process, fill a jerry can for their own personal use or even siphon a small amount of fuel off the top of a tank but on a regular basis. Due to the relatively small theft or discrepancy, the crime can understandably go undetected for some time.

Fuel theft solutions

ANTI-SIPHON DEVICES

Anti-siphon units are devices used to combat common methods of fuel theft. They fit directly into the fuel filler neck and repel the use of siphoning tubes. Advanced anti-siphon devices also defend against skimming, usually with a floatation mechanism that prevents fuel accessing the filling chamber, which could otherwise be reached. Some systems are also provided with the option of a locking cap to provide an additional barrier to entry.

FUEL ALARMS

Generally for use on HGV's, fuel alarm systems monitor the fuel tank when the vehicle is not in use. Utilising specially engineered sensors that detect specific attacks to the tank itself (such as tank piercing or attacks to the locked fuel cap), alarm systems can provide an effective deterrent against such attacks. Alarms generally offer automatic arming (once the ignition is switched off) and also have the option for external LED's that flash continuously to deter thieves, a proven technique in crime reduction which can reduce the likelihood of attack. In the event of an alarm event users can select between a traditional siren and/or send an alert via GSM or tracking system.

FUEL MANAGEMENT SYSTEM:

Fuel management systems provide more detailed information about fuel usage, providing early warning indicators in the event of unusual activity. Monitoring fuel flow, fuel-level indicators, filler cap opening, and general fuel usage statistics can provide a comprehensive level of fuel data. The telematics-based technology transmits real-time information, which, in turn, is analysed to provide notifications of any discrepancies or potential misuse for further investigation.
Fuel management systems that incorporate highly accurate fuel-level indicators are particularly insightful and can help to detect any regular skimming of fuel.

Guarding against fuel theft

Be Proactive:
Monitor fuel usage in every vehicle within the fleet, compare MPG data, and identify any inconsistencies; even if you do not suspect your employees of fuel theft, monitoring fuel usage is good practice. In the worst-case scenario you may be able to identify an opportunity to improve driver performance.

Site Security:
Perimeter fencing, CCTV and security lighting will act as a deterrent, reduce opportunity, and assist in capturing evidence if you suspect foul play by either employees or third parties.

Educate Drivers:
Make your employees aware of the impact that fuel theft can have on the company and what the individual consequences would be if caught carrying out fuel theft. By raising the profile of the subject and making employees aware of the fact it is being actively monitored may be sufficient to deter anyone from engaging in such activity.

Fuel Management and Monitoring Systems:
Consider investing in fuel management systems that provide greater insight into how fuel is being used across the organisation. They stop unauthorised use, allow easier management of stock, track usage, restrict driver access, and help you to identify any anomalies.

Security Devices:
Consider additional security such as fuel alarms, lockable fuel caps, anti-siphoning devices, and fuel-sender protectors, all of which guard against potential fuel theft.

Defensive Parking:
Park vehicles in a way that protects and blocks access to fuel tanks. This can add another layer of difficulty that may deter thieves and cause them to move on to an easier target. If parking in lay-bys, ensure that the fuel tank is exposed to the traffic, thus making it more difficult for the thief to stay hidden.

Chapter 16:

THE MIGRANT THREAT

Clandestines using vehicles to try to cross borders undetected is not a new phenomenon. However, over the course of the last few years it has gathered alarming momentum, arriving at the point at which we are now facing a crisis situation. It creates a whole new set of pressures and concerns for road transport operators and quite possibly leaves many questioning what exactly is the haulier to do and what are their legal obligations.

A perfect storm

The 'perfect storm' of civil unrest, war, famine, terrorism, pestilence and poverty has facilitated a crisis situation at ports and border points. For operators who must cross borders it is a struggle that has been present for many years, but one which intensified in 2014/15 and shows no sign of abating.

The perilous situation has pushed some haulage companies to the brink, caused disillusioned drivers to turn their backs on an industry with which they have been involved for their entire career, and induced a staggering £16 million in fines in just three years (after clandestine entrants were found concealed within a vehicle).

There remain calls from within the road transport industry for authorities to do more to protect hauliers and, more specifically, drivers who have increasingly become the victims of more aggressive attacks, as tension amongst those attempting to cross the border illegally intensifies. But remarkably, as many as one in two vehicles negotiating these borders do not have even basic security measures in place to protect load areas. A phenomenal revelation when it is considered an estimated £1 billion in spoiled loads is being thrown away every year by UK businesses.

Whilst the recent closure of the Calais migrant camp has eased the situation somewhat, this is likely to offer nothing more than temporary respite and, in some respects, only serves to widen the threat across a larger geographical area as the threat disperses.

It is a scenario that requires a collaborative approach to effectively combat what can be equally a delicate yet violent situation. For their part, hauliers and logistics providers must protect their own interests and commit to providing viable, more secure services.

Fines issued to both hauliers and drivers have increased dramatically since 2014

Haulier & driver obligations

If you do not correctly secure your vehicles or take adequate precautions to prevent infiltration, both you and your drivers are liable for fines of up to £2,000 per entrant that you carry (into the UK), under the Immigration & Asylum Act 1999 (Section 32)..

The legislation is applied only to those who carry entrants to the UK as a result of negligence or carelessness. If clandestines are found in a vehicle and carriers can demonstrate that they have employed an effective system to prevent clandestine entry or can point to mitigating circumstances (i.e. duress), a person or company shall not be liable for a penalty.

Border Force provides a full code of practice to help operators of commercial vehicles to meet their obligations to provide an effective system to prevent the carriage of clandestine entrants. It covers the key areas that hauliers must address, including when and how frequently load areas must be checked, the correct use of seals (or sealing devices), required documentation, recording of security checks, and what to do in the event of a suspected security breach. To read the full code of practice, visit www.gov.uk/government/publications/civil-penalty-code-of-practice-prevention-of-clandestine-entrants

SUMMARY OF HAULIERS' REQUIREMENTS

1. Hauliers are required to make provision for the use of robust security devices to effectively secure the vehicle, load and load space (seals, locks, TIR Tilt Cords).
2. Provision for driver training on how to use the system and associated security devices.
3. Provision for written instructions for drivers on how to use the system.
4. Provision for checklists carried in the vehicle for the driver to follow and complete.
5. Implement a system to monitor that checklists are being completed.

CIVIL PENALTY ACCREDITATION SCHEME

Road haulage companies can protect themselves further by signing up to the voluntary 'Civil Penalty Accreditation Scheme'. It has been set up to aid companies in reducing the risk of receiving fines by ensuring that they have an effective system in place to reduce clandestine entrants. For more details, visit www.gov.uk/government/publications/civil-penalty-accreditation-scheme/civil-penalty-accreditation-scheme.

WHAT IS EXPECTED OF THE DRIVER

Border Force have also issued a guide for drivers, which details their responsibilities, what can be done to safeguard against clandestine entrants, and any potential fines for which they may otherwise be liable. The full guide can be found at www.gov.uk/government/publications/guidance-for-hauliers-on-preventingclandestine-entrants

Guarding against the threat of clandestine entrants

Clandestine Policy:
Put a policy in place for drivers so that they know what is expected of them when negotiating borders. Two in five companies involved with cross-border logistics do not have such a policy. Most importantly, instruct drivers on what to do in the event that they suspect persons may be concealed within the vehicle.

Exclusion Zones:
Consider introducing exclusion zones, advising drivers that they must not stop within a certain distance of a port/border (even for fuel).

Rest Breaks:
Identify suitable, secure truck stops where drivers are able to stop for rest breaks.

Park Securely:
Encourage drivers to consider parking on the opposite side of the carriageway, which may give the impression that vehicles are heading away from a port.

Preventative Security Measures:
Ensure that you are taking adequate measures to secure your vehicles against the potential for clandestine entry. Review whether the preventative security measures used in your vehicles are sufficient to withstand unauthorised entry.

Early Warning:
In addition to physical security measures, also consider door open warning systems that provide immediate notification in the event of unauthorised door openings.

Code of Practice:
Ensure that you are following the code of practice for the 'Prevention of Clandestine Entrants' and that you are meeting minimum criteria for an effective system.

Accredited Carriers:
Consider joining the 'Civil Penalty Accreditation Scheme', which protects you against fines (in the event that clandestines are found on board a vehicle).

Contingencies:
Ensure that contingency plans are in place if certain routes or ports become difficult to negotiate (i.e. during strike action).

How clandestines target vehicles

LOAD DOORS

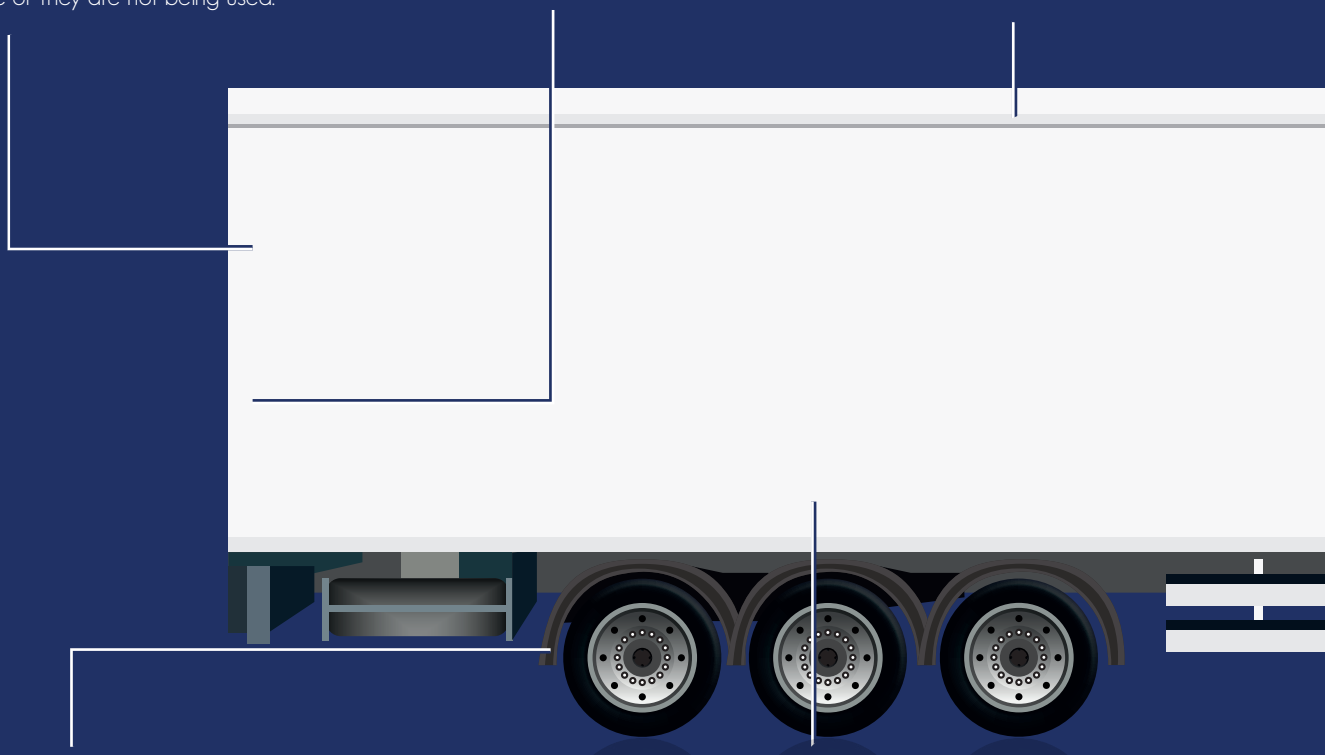
The most common entry point targeted by migrants. Surprisingly many carriers fail to sufficiently protect this vulnerable area with Border Force claiming that around half of all commercial vehicles do not have security measures in place or they are not being used.

SEALS / PADLOCKS

Basic applications such as disposable seals and padlocks can be easily defeated and even manipulated to give the impression they have not been breached.

ROOF HATCHES

Clandestines will go to extraordinary lengths to avoid detection. There have been a number of cases where people have been found hiding in tankers carrying hazardous loads.



VEHICLE AXLES

Arguably this method, over any other, highlights the extreme measures that migrants are willing to employ in their bid to reach the UK. Migrants often target junctions where vehicles stop before climbing aboard the axle and desperately clinging on – sadly this method has resulted in numerous fatalities.

CURTAINS

It is accepted that most migrants attempting to board vehicles will carry knives or other cutting implements, thus soft sided vehicles are particularly susceptible to clandestine entry – more organised attempts will also see the temporary repair of the curtain in a bid to remain undetected.

There is little bias with regards to the type of lorry or trailer targeted by clandestines, stowaways are regularly found in lorries with hard-sided bodies, curtains and refrigerated units. There have even been cases where stowaways have been located inside tankers carrying chemicals.

As attempts by clastendines to break into the UK have increased, regrettably so too have the number of reported fatalities, compounded by a shocking case in August 2015, when more than 70 clandestines were found suffocated inside an abandoned refrigerated vehicle in Austria.

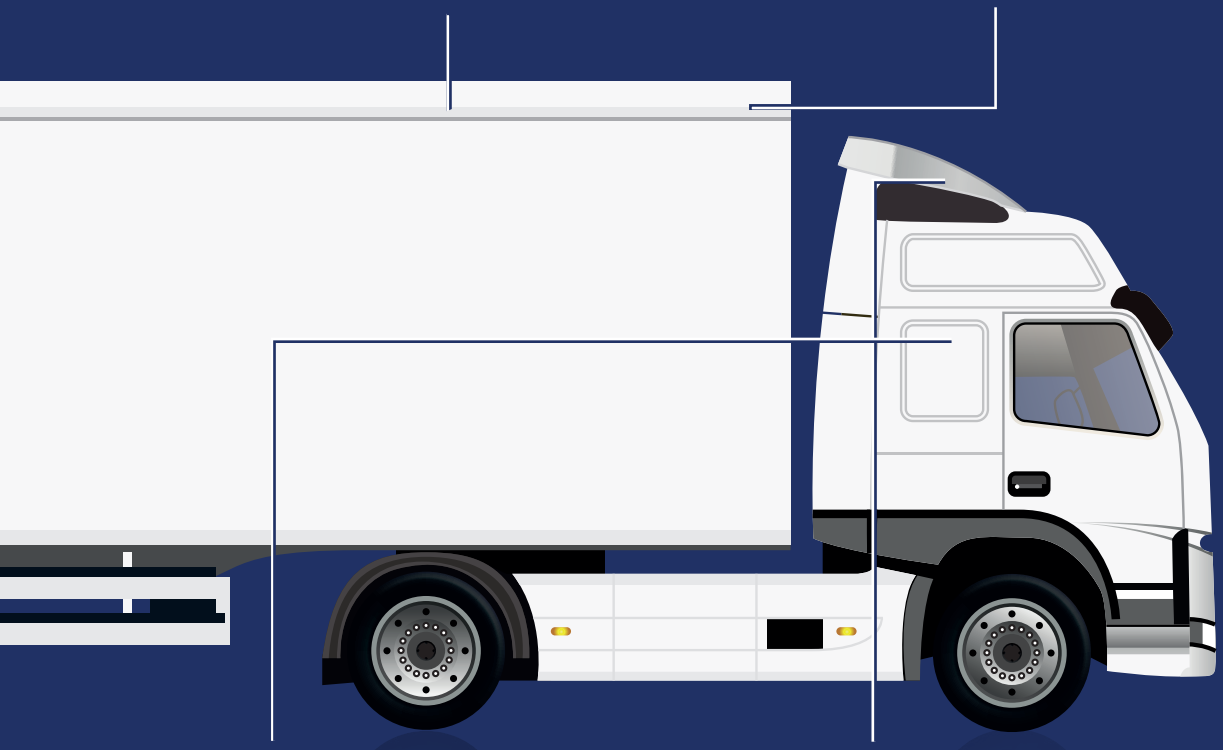
The diagram below shows typical areas on a commercial vehicle that are targeted by stowaways. These areas should, as a minimum form part of a drivers visual checks each time they stop.

ROOF ACCESS

The roof is yet another location exploited by clandestines. When attempting to board a vehicle clandestines have been known to cut holes in the roof, to drop down and conceal themselves within the load area.

ROOF

There have been various sightings and cases whereby migrants quite simply hitch a ride on top of a vehicle itself by lying down and clinging on to the roof.



STORAGE LOCKERS & PANNIERS

Migrants are ever more resourceful when attempting to conceal themselves aboard vehicles. Storage lockers and even pallet carriers (or panniers) are being increasingly targeted, particularly when drivers stop at rest areas or fuel stations.

WIND DEFLECTORS

The concealed location provides a 'perfect' hiding place that can be easily missed if not correctly inspected, allowing stowaways to go undetected.

Summary – How do we move forward

'The sad reflection on our society is that the losses and cost of commercial vehicle crime is now more costly than ever.

The fight against commercial vehicle crime is a constant running battle especially over the last number of years when HGV's have been the targets of highly organised criminal gangs. Fortunately we now have more awareness and a much stronger army of people and organisations fighting together with modern technology to contain and hopefully reduce the problem.'

Not my words, but those of my father, Jim Maple; writing in a commercial vehicle security guide that was published in 2000 (titled 'The Big Blue Book.') I could write a similar conclusion today and it would still hold true. It would be unfair and indeed inaccurate to say that we have not made progress in the fight against cargo criminals but equally it is important that we face up to the fact that whilst the industry has not stood still, nor have the criminals, they can be ingenious, sophisticated and bold...and that is a heady cocktail to counteract.

So just how do we move forward? How do we reduce supply chain losses and commercial vehicle crime?

In many ways, the industry finds itself in a classic catch 22 situation.

Profit margins for road transport operators are notoriously low, hovering around the 4% level, consequently there is a relentless pursuit to keep overheads and costs low. Specification of enhanced security measures or implementation of additional procedures increase costs, a barrier which many cannot or simply do not have the appetite to overcome.

In an increasingly crowded and fiercely competitive market, insurance companies must also fight to stay competitive and do not wish to insist or impose additional security measures upon clients, which could consequently jeopardise contracts, relinquishing business to competitors who perhaps will cover the risk without the additional security measure.

Finally, the manufacturer / shipper, wishes to deliver the goods to their customer at the most competitive (lowest) cost, by the most economical means. The manufacturer therefore, knowingly or not, is unwilling to pay a premium to a carrier who has invested in a more secure fleet.

IMPROVING THE SITUATION

One would assume the party who experiences the biggest losses would be the most active in improving security measures to reduce the associated impact. However, unsurprisingly this is perhaps a little simplistic, let us consider the following.

If we first look at the transport company; they tend to work on a standard insurance cover based on weight, with no particular regards to the exact value of the cargo they are carrying. The effect of this is their losses are not a true representation of the problem.

The insurance companies who cover the risk of cargo, tend to be global companies who cover the risk from point of manufacture to point of sale. Thus, insurance cover may encompass transport via sea, air, rail, and road and the risk is therefore greater. Quite often these are large annual premiums, covering large blue chip manufacturing companies, for large sums of money. In the event of a loss, it may often be quite insignificant when considering the entire contract and scale of the yearly premium charged for such cover.

Add to this that the losses are not always seen on a local level and that the manufacturers losses can often be offset by their own self insurance fund and that of the insurance company, who are underwriting the remaining portion; so consequently individual cases of loss are not always large enough to cause sufficient concern when compared to annual turnover.

Finally, with mass globalisation and the ferocious pace of e-commerce, shrinkage is seen in some quarters as

merely an unsavory by-product. Previously, when manufacturers were smaller, production was a more localised affair, so to the carrier and insurer of the goods would be provided by a local organisation. In the event of any losses the associated impact was intensified for all concerned. The loss values represented a much greater proportion of a companies turnover and consequently the desire, indeed the requirement to improve security was perhaps greater in years gone by than it is today.

As companies become bigger and decisions global, in turn the risk is covered by global insurance companies. Losses incurred in one region are not always immediately visible, nor is their impact as intense as it once may have been across the entire organisation.

Perhaps the most pertinent example of this can be demonstrated by vehicle manufacturers. A vehicle producer may be experiencing a spike in theft or break-ins in a particular region or country. Quite understandably this would result in an outcry in said region to improve their security offering on their vehicles. However in the scale of the number of vehicles they sell around the world and lack of problems in other countries, the associated business case does not justify the additional cost to make improvements.

Legislation often is the only answer to improving security and safety. However governments would only implement such measures if it is felt necessary due to public safety or it is in their best interests, as was the case with the legislative requirement to provide electronic immobilisation on all new vehicles back in the last millennium.

It is difficult to foresee any imminent security cases that would lead to government intervention. Perhaps it could be argued that if commercial vehicles are being used to smuggle people across borders, or it was established beyond any doubt that the proceeds of truck crime, were funding greater and far more serious crime such as terrorism. Alas, it is unlikely such steps would be taken any time soon.

DOES THE PURSUIT OF PROFIT PROVIDE THE ANSWER

'So, just how do we move forward? How do we reduce supply chain losses and commercial vehicle crime? There is no single movement that is likely to initiate an immediate improvement in vehicle security or reduction in cargo crime. Organisations such as TAPA and in the UK the RHA security committee, have no doubt been positive drivers in raising awareness and providing a platform to move security of goods in transit forward. But it should be remembered that they are entirely voluntary; often the pressures of commerce mean that even their own members and greatest supporters do not always follow the best practices that they try to encourage. Other factors such as contractual obligations and implications of load infiltration (at borders) may also encourage carriers to increase security but the motivation for carriers to voluntarily improve in transit security is low.

Perhaps the irony is that commerce and the pursuit of competitive advantage, may just be the saving grace. In the same way that companies may utilise an environmental agenda to strengthen a brands position, so to a security strategy where forward thinking companies take proactive steps to voluntarily reduce losses, could provide the platform for a mutually beneficial scenario.

It is also essential we work together in a common agenda, only with a collaborative approach, where the cheapest price is not always victorious will we truly make any significant strides.

As my father concluded back in 1998 'Will we ever win the fight against commercial vehicle crime? The answer has to be NO, not completely. But what we do have is more awareness and a much stronger army of people and organisations fighting together with technology to contain and hopefully reduce the problem.'

In the end the pursuit of profit will perhaps win through and shape our future in cargo crime, as in all things in life...

CART Security Guide Working Group

PAUL NUNN - Marketing Manager

A marketing professional who has worked in the commercial vehicle sector for more than 10 years. Paul currently holds the position of Marketing Manager for commercial vehicle and logistics security specialist, Maple.

Passionate and enthusiastic about promoting and supporting security best practice within the logistics industry, Paul has acted as project leader and author for the 'CART Security Guide,' nurturing the original concept from the formulation of the working group, right through to the subsequent publication being realised.

ALAN MAPLE - Technical Director

Having followed in his Fathers footsteps with a passion for engineering, Alan joined the family business as an installation engineer. He soon progressed into a technical sales role with a real enthusiasm for developing solutions to solve customers safety and security problems.

During his 37 years of industry experience, Alan has been responsible for designing and patenting a plethora of commercial vehicle safety and security applications, won a motor transport award for innovation (for developing a life saving safety product) and has been invited to contribute to various security committees. Alan's most recent innovation saw the development of the first certified locking system for the aviation retail industry..

ANDREW ROUND - Industry Liaison and Intelligence Sharing

A well respected freight crime specialist who currently works as an Intelligence Officer/ Industry Liaison Officer for NaVCIS Freight Desk (National Vehicle Crime Intelligence Service), concerned with all organised freight crime in the UK.

A retired West Midland Police Detective with 16 years experience in Organised Freight Crime investigation and intelligence, including Op.Indicate from 2003 to 2006, which successfully targeted and convicted a West Midlands Organised Crime Group. Andrew, took over the running of the National Freight Crime unit TruckPol in 2007 from the Met Police,when NaVCIS was formed under ACRO (Criminal Records Office), now operating as part of the NPCC (National Police Chief's Council).

ANDY SCOTT Dip CSMP

- Head of Security & Operational Resilience, UK, Ireland, Nordics & Baltics

Andy has worked in the security industry for over 20 years focusing mainly on the Financial and Logistic sectors. He currently holds the post of Head of Security & Operational Resilience at DHL Global Forwarding, with responsibility for UK & Ireland, Nordics & Baltics.

Andy is Vice Chairman of the RHA Security Forum and was, until recently, Chairman of the Carrier Intelligence Group, a position he held for nearly 10 years. He is a serving Special Inspector in the Metropolitan Police Special Constabulary, a role he has undertaken for over 18 years.

CHRYS RAMPLEY FAIRSO MILT MInstTA

- Manager, Infrastructure, Security & Business Affairs

Chrys has been working in the freight industry for the past 39 years, 20 of those at the Road Haulage Association. Throughout that time she has developed and managed a wide range of crime reduction and road safety initiatives in partnership with the Police and the charity, Crimestoppers. More recently she has been involved in the European projects of SETPOS and LABEL in campaigning for improved parking facilities for drivers across Europe.

Prior to that Chrys worked in shipping as the Freight Operations Manager for Sealink at the port of Dover followed by a four year spell at Eurotunnel, two years prior to its inauguration, setting up the toll system and two years after in freight customer services..

CHRIS HOLLAWAY - Founder & CEO

Beginning his career 20 years ago delivering wardrobes in box vans, to managing teams of drivers delivering pressurised hydrogen to Nuclear power stations, Chris Holloway gained his experience both on and off the road.

Passionate about the industry, he created MotorwayBuddy, a smart phone application and haulage company tool that all sectors of the road transport industry can utilise. Currently working with Police and crime organisations highlighting crime hotspots throughout the UK, assisting haulage companies to simplify payments and most importantly helping drivers to establish where is safe to park, Chris continues to thrive on solving the haulage industries problems..

MICHAEL SAUNDERS - Regional Security Manager (South) UK & Ireland

Michael is employed as a Regional Security Manager for DHL Global Forwarding having retired from the Metropolitan Police after 31 years' service. He is also an active member of both the RHA Security Forum and was a member of the Carrier Intelligence Group.

During his police service Michael was involved in many high profile investigations and was a part of Operation Grafton – the MPS Unit responsible for investigating serious, organised and high value crime committed in and around Heathrow Airport and the Home Counties.

PAULE MAYOH MILT - Consultant Risk Surveyor

An experienced risk management practitioner, with particular expertise in logistics, supply chain integrity and transportation. Paule's expertise is founded on 27 years of experience in the insurance, logistics and supply chain industries, much of which has been at a senior level.

An expert in both B2B and B2C operations, haulage, warehousing, (dedicated, shared user and cross dock operations) and an accomplished and experienced insurance loss investigator and pre / post risk surveyor. Paule is a full member of the Chartered Institute of Logistics & Transport and represents RSA at TAPA Conferences, the RHA Security Forum and as a committee member of the Distribution Industry Partnership Scotland [DIPS].

STEWART HURRY - Resilience Manager

Stewart retired from Police Scotland in 2014 after 30yrs service, joining SBRC in May 2015. During his 30 years with the police Stewart had experience in the areas of crime prevention, safer communities and violence reduction.

On joining the centre, Stewart took over Project Management of the Distribution Industry Partnership Scotland (DIPS), a group of companies involved in the production, freight forwarding and distribution of spirits, produced in Scotland. In addition to focusing on the safety and security of freight, Stewart also leads the work of the SBRC in respect of the passenger transport sectors also. A current major project is the identification and development of a network of secure parking locations across Scotland.

References

ARTICLES / JOURNALS

Army Sustainment: How to Chose and Use Seals (2012)

Association for European Transport and contributors: Secure Truck Parking Areas: Fighting Crime and Increasing Safety (2007)

BSIA (British Security Industry Association): Lone Workers - an employers guide (Form No 288. Issue 1, February 2010)

BVBA Wim DEKEYSER 2017: Statistic Data: Thefts of Cargo Crime in Belgium (2017)

European Parliament, Policy Department, Structural and Cohesion Policies: Organised Theft of Commercial Vehicles and their Loads in the European Union (July 2007)

Europol: Cargo Theft Report, Applying the Brakes to Road Cargo Crime in Europe (2009)

FALCON (Fraud and Linked Crime Online): Protect Briefing 17/03/17 (March 2017)

Freight Best Practice Scotland: Lorry Parking Guide (January 2011)

FWI (Freightwatch International): Pharmaceutical Cargo Theft in Europe (2016)

FWI (Freightwatch International): Putting a Price Tag on Underreported Cargo Theft in Europe (2016)

FWI (Freightwatch International): EMEA Cargo Crime Intelligence Update Q4-2015 & Full-Year-2015 Snapshot(2016)

FWI (Freightwatch International): 2013 Global Cargo Theft Assessment (2013)

G4S: Intelligence Bulletin: Criminal use of Additive Manufacturing (3D Printing) in Cargo Thefts

PSDB (Policer Scientific Development Branch): Publication No 14/99 Guidelines for Roof Markings on Heavy Goods Vehicles (1999)

HomeOffice, JAGOLT LL01: Steer Clear of Truck Theft (2007)

Journal of Transportation Security: Theft of Pharmaceuticals in Europe (October 2015)

NaCTSO (National Counter Terrorism Security Office): NaCTSO Guidance Note SA/2015: Reviewing your Protective Security

NCIS (National Criminal Intelligence Service). The Threat to the United Kingdom from Road Freight Crime (2005)

RHA (Road Haulage Association): What to Look for at VOSA Roadside Stops

RHA (Road Haulage Association): RHA Operators Handbook (2017)

RSA (Royal Sun Alliance): Marine Risk Management, How to Vet New Employees (December 2009)

Styles and strategies of learning. British Journal of Educational Psychology, 46, pp. 128-148.

SOCA (Serious Organised Crime Agency) - Lorry Crime Prevention (April 2011)

TAPA (Transported Asset Protection Association): Romanian M.O. - A Growing Concern? (May 2014)

TAPA (Transported Asset Protection Association): Incident Information Service Annual Report (2016)

The Treasurer: Supply Chain, The Weakest Links (September 2008)

Vigilant (Transported Asset Protection Association) Threat to Supply Chains posed by Stowaways Expected to Lead to Increase in TAPA TSR Certifications (June 2015)

Zurich Insurance Group Ltd: RiskTopics - Cargo Theft in Europe (July 2015)

BOOKS

Knapper, C.K. and Cropley, A. 1991: Lifelong Learning and Higher Education. London: Croom Helm.

WEBSITES & ONLINE ARTICLES

HSE (Healty and Safety Executive): Working Alone. www.hse.gov.uk/pubns/indg73.pdf. Accessed 31/03/17

Cargo Security Alliance: Cargo Theft by Fictitious Pick-up. www.securecargo.org/news/csa-white-paper-cargo-theft-by-fictitious-pick-up. Accessed 08/03/16

Commercial Motor: The Curtain Slashers. www.commercialmotor.com/news/the-curtain-slashers . Accessed 31/03/17

Lloyds Loading List: UK Supply Chain 'in danger of collapsing,' warns FTA: www.lloydsloadinglist.com/freight-directory/news/UK-supply-chain-%E2%80%98in-danger-of-collapsing%E2%80%99-warns-FTA/62946.htm#.WOIxRzF1qUk. Accessed 30/06/16

Food Manufacture: Millions of Pounds of Food Wasted by Calais Crisis: www.foodmanufacture.co.uk/Supply-Chain/Millions-wasted-as-food-falls-victim-to-migrant-chaos. Accessed 30/06/2016

LogistIQ Insurance Solutions: How to Avoid Cargo Theft by Fictitious Pickup: www.logistiqins.com/how-to-avoid-cargo-theft-by-fictitious-pickup/. Accessed 08/03/16

SMMT: Stolen vehicles down 70% www.smmt.co.uk/2015/04/stolen-vehicles-down-70-in-a-decade-as-smmt-calls-for-more-detailed-theft-tracking/. (Accessed 03/04/17)

Thatcham Research Centre: Theft Without Keys www.thatcham.org/files/pdf/Theft _Without _Keys.pdf. Accessed 16/04/16

The Texas Department of Insurance: Truck Hijacking Prevention Factsheet www.tdi.texas.gov/pubs/videoresource/fsprotecttrucks.pdf. Accessed 01/03/17

Tracker: Only One Third of Stolen Ford Transits are Recovered. www.tracker.co.uk/news/press-releases/only-one-third-of-stolen-ford-transit-vans-are-rec. Accessed 04/04/17

University of Leicester Standing Committee of Deans (6/8/2002) Internet code of practice and guide to legislation. www.le.ac.uk/committees/deans/codecode.html. Accessed 8/8/02

ACKNOWLEDGEMENTS

The working group would like to extend their thanks to Paul Nunn for all the extremely hard work he has put in to producing this guide. He would likely comment that 'this is my job,' however, like all the members of the working group, this has become his passion, and without that we are certain it would have taken much longer for this guide to reach print and to meet the required standard.

Printed in the United Kingdom. Maple Fleet Services, 2017

Maple Fleet Services, Maple House, Crown Royal Industrial Park, Shawcross Street, Stockport, SK1 3EY, UK

www.maplefleetservices.co.uk

The CART Security guide has been produced in collaboration with a working group, made up of industry professionals representing the following companies and organisations;

Maple
info@maplefleetservices.co.uk
0161 429 1580
www.maplefleetservices.co.uk

NaVCIS; National Vehicle Crime Intelligence Service
freight@navcis.pnn.police.uk
02380 479 305
www.navcis.police.uk

DHL Global Forwarding (UK) Limited
08444 771 100
www.dhl.co.uk

Road Haulage Association
weybridge@rha.uk.net
01932 838 905
www.rha.uk.net

Motorway Buddy
info@motorwaybuddy.com
0161 956 3500
www.motorwaybuddy.com

RSA - Marine Risk Management
rod.johnson@uk.rsagroup.com
0207 337 5287
www.rsabroker.com

DIPS – Distribution Industry Partnership Scotland
DIPS@sbrcentre.co.uk
01786 447 441
www.sbrcentre.co.uk