

vigilant

THE MONTHLY CARGO CRIME UPDATE FOR TAPA'S GLOBAL FAMILY

THINK TAPA

Are you unlocking all of the benefits
of your TAPA membership across your
end-to-end supply chain?

Page 3: Top speakers line up for TAPA EMEA's Dublin conference

Pages 4-5: Are you embracing TAPA's DNA and making the most of your membership?

Page 6: Eye-on-Tech looks at the latest supply chain security technology news

Page 7: Using the Incident Information Service (IIS) to manage risk

Pages 8-12: The inside job – the 'common vulnerability' within your business

Page 13: FSR, TSR and PSR certifications on the up in EMEA

Pages 14-15: TAPA APAC on the role of Manned Guarding in 'Belt & Road' initiatives

Pages 16-17: A look back at TAPA Americas' T1-Meeting in Atlanta

Pages 18-22: Cargo Crime Monitor for EMEA plus the latest supply
chain losses news for June from EMEA and APAC

Page 23: A round-up of the latest companies to adopt TAPA's Security Standards

Pages 24-25: Standards FAQs answers more of your certification enquiries

Page 26: Meet the Board - James Neville, TAPA Americas

Page 27: Welcome the latest new members to join the TAPA Family

TRANSPORTED ASSET PROTECTION ASSOCIATION

welcome

A SHINING LIGHT IN INTERNATIONAL SUPPLY CHAIN SECURITY



This month, we make no excuse for reminding you of the benefits of your TAPA membership.

We naturally hope this won't come as big news to you because you are already participating in our Security Standards programme, using our incident intelligence to manage risk, attending TAPA training events, and networking at our global events.

The main reason for reminding you is to encourage you to share this information with your business partners, industry associates and suppliers that you feel can also gain from joining the growing TAPA Family. You can connect them directly with our regional administration teams or direct them to our website to find out more. Every new member makes us stronger.

In this issue, we look at many of the latest developments to benefit the TAPA Family. Members who have already registered to attend TAPA EMEA's Dublin conference in October will see that they can look forward to another information-packed agenda and insights from leading experts from businesses

including Ahlers, Boehringer Ingelheim, F.Hoffmann-La Roche and Solvay. Our friends in TAPA Americas also reflect on the outcome of their latest T1-Meeting in Atlanta.

We also consider the growing risks from employees inside companies and consider the phenomena of the 'Internal' M.O. as seen through the expert eyes of BSI and the TT Club.

As our Security Standards continue to grow in terms of global certifications, TAPA APAC bring us up-to-date with the region's Guarding Security Requirements, while our Standards FAQs answer more of your questions as you prepare for the revised 2020 versions of our Facility Security Requirements (FSR) and Trucking Security Requirements (TSR). Regular visitors to our IIS database will also have seen the recent update to the incident icons which appear on our mapping tool to make our cargo crime intelligence even easier to navigate.

We also reflect on some of the latest high value and high risk incident news from countries around the world as we report another month of losses from supply chains of millions of Euros – always the biggest reminder of all of

the challenges we face and the reason why more and more Manufacturers, Logistics Service Providers and other supply chain security service providers want to be part of our Family.

In the last month, another 18 companies have joined TAPA in the Americas, Asia Pacific and EMEA. That's an average of more than one new member every two days. You can help us to grow this even further.

There has never been a better time to join our Association and the benefits we offer will continue to grow. Let's spread our message and awareness all over the world.



Marcel Saarloos
Chairman,
TAPA EMEA



DUBLIN CONFERENCE TO FOCUS ON END-TO-END CORPORATE SECURITY, RISKS TO PHARMA SUPPLY CHAINS AND DOING BUSINESS SECURELY IN RUSSIA

With three months to go to TAPA EMEA's conference in Dublin on 23 & 24 October, the first group of expert speakers and panellists has been announced for what promises to be another information-packed event for delegates focused on end-to-end supply chain security.

On the first morning, Werner Cooreman, Group Security Director of Solvay, and Lutz Wohlfahrt, Head of Corporate Security and Crisis Management at Boehringer Ingelheim Corporate Center GmbH, will participate in the Chief Security Officer Panel Discussion looking at '*Why is a supply chain security programme so crucial for an end-to-end corporate security strategy?*'.

The afternoon session on day one will also include a case study on managing risks in Russia, presented by Stefan Van Doorslaer, CEO of Ahlers Group and Chairman of the Executive Committee of the St. Petersburg International Business Association (SPIBA).



Delegates will also hear a case study from F.Hoffmann-La Roche Ltd, presented by the company's Global Logistics Security Officer, Ulrich Gläsemann. He will discuss the risks facing a typical supply chain in the pharmaceutical industry as well as best practices and emerging trends. He will also explain how Roche manages Logistics & Security Risks using TAPA's Security Standards, complemented with additional pharma-specific requirements.

More presentation topics, speakers and panellists will be announced in the coming weeks.

Attending the conference will also enable members to get the latest updates on the

progress of TAPA's 2020 strategy, presented by TAPA EMEA's newly-appointed President & CEO, Thorsten Neumann, and the countdown to the next 2020 revisions of the Association's Facility Security Requirements (FSR) and Trucking Security Requirements (TSR).

With over 150 delegates already registered, if you have yet to confirm your place at the conference, it is important to do so as quickly as possible. Communications have been sent to all TAPA EMEA members with a link to the Dublin conference registration system.

If you are interested in any of the remaining sponsorship opportunities available in Dublin, please contact Claudia Kusche at conferenceteam@tapaeMEA.org



VEDA AUTOHOF SYMPOSIUM TO HEAR TAPA'S VIEWS ON SECURE PARKING

Thorsten Neumann, President & CEO of TAPA EMEA, will be one of the panellists discussing the need for more secure parking for trucks to improve supply chain security at the VEDA Autohof Symposium in Berlin on 26 September. He will be joined on the panel by experts from law enforcement agencies and government as well as Parking Place Operators.



TAPA 'DNA' BUILDS RESILIENT SUPPLY CHAINS

Are you maximising the value of your TAPA membership to help manage risks and to increase the resilience of your supply chains? This infographic provides a quick reminder of the end-to-end supply chain security solutions TAPA delivers and which are available now for every member of the Association ...



TAPA SOLUTIONS ...

INCIDENT INTELLIGENCE

TAPA's Incident Information Service (IIS) provides the latest cargo crime intelligence reported to the Association and is a database of over 30,000 incidents members can review to increase their understanding of when, where and how incidents are occurring and the products being targeted.



SECURE FACILITIES

Developed by the industry, TAPA's Facility Security Requirements (FSR) are respected as the leading Security Standard to protect warehouse operations, distribution centres and storage facilities.



SECURE ROUTES

TAPA's IIS mapping tool enables members to plan secure transportation routes by highlighting the number and types of cargo crimes along their intended routings, ensuring they avoid incident 'hotspots' where offenders are most active.



... DESIGNED
TO MANAGE
GROWING RISKS



MORE DATA

TAPA's IIS recorded 3,981 cargo crimes in the EMEA region in 2018, up 38.2% year-on-year and a growth of 261.2% over the last five years. Losses last year exceeded €153 million - yet, still, most losses from supply chains go unreported.



MORE CERTIFICATIONS

With TAPA Facility Security Requirements (FSR) certifications now at their highest level in the Association's history, only 1.1% of crimes reported to TAPA EMEA in 2018 were Theft from Facility incidents.



MORE INSIGHT

TAPA's cargo crime database shows the geography of cargo crimes, including GPS coordinates to help Manufacturers and Logistics Service Providers pinpoint areas to avoid.



SECURE TRUCKING

The number of TAPA Trucking Security Requirements (TSR) certifications in the EMEA region rose by 33.9% in 2018 as more companies used the Security Standard as an effective way to protect their vehicles, drivers and customers' products in transit.



95%

MORE FACTS

High value, theft targeted products - which today include virtually all goods - are most at risk when they are onboard transport and logistics vehicles. In EMEA in 2018, over 95% of all recorded losses involved thieves targeting trucks.

SECURE PARKING

TAPA's new Parking Security Requirements (PSR) is a Security Standard developed by Manufacturers and Logistics Service Providers for Parking Place Operators and aims to build a network of secure parking sites for trucks. Already, in the first weeks of the programme, over 4,500 parking places have been added to the TAPA secure parking database in 10 countries in EMEA, with more rapid growth expected.



60%

MORE SUPPORT

In 2018, nearly 60% of cargo losses involved thieves targeting trucks which had stopped in unsecured parking places, such as roadside laybys, industrial estates and motorway service areas. TAPA's PSR programme will make members' supply chains more secure.

GLOBAL CONNECTIONS

SPECIALIST TRAINING

TAPA's team of training specialists provide courses which help members to begin or grow their use of the Association's FSR and TSR Security Standards to make the certification process as efficient and seamless as possible.



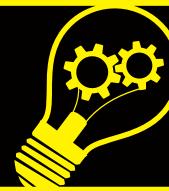
MORE ENGAGEMENT

TAPA's conferences in the Americas, Asia Pacific and Europe, Middle East & Africa regions are unique networking opportunities, offering the chance to engage with risk management specialists and gain new contacts.

MORE EFFICIENT

TAPA is developing online training solutions to give members faster, more convenient and lower cost access to its training programmes and those of its partners.

EYE-ON-TECH



Percepto Drones

Percepto's autonomous drone stations provide industry teams with a continuous stream of aerial data made available at critical moments to key personnel. All industrial companies engaging in digital transformation and intelligence initiatives can benefit from easy-to-use and invaluable real-time insights provided by their autonomous drones, without the availability constraints or cost burden of services provided by human operators. An on-site autonomous drone system for improving facilities' security and operations, the solution offers fence patrol, suspect detection and tracking, discovery of safety hazards and inspection of infrastructure and equipment. The entire operation cycle is fully autonomous with pre-defined schedules and no need for a human pilot, and supports 24/7 operations with data collection around the clock, the company says.

To learn more, go to www.percepto.co

Convexum – preventing drone attacks

Convexum's proactive counter-drone solution claims to prevent intrusions into private airspace by automatically taking over and safely landing the drones in a predefined location. Convexum is the only solution on the market to effectively deny take-off from within the protected perimeter. The end-to-end system does not use firearms or RF jamming, ensuring no collateral damage, and includes actionable alerts, drone location display and smart handling. For selected drone models, Convexum is also able to record the operator's last known location. Features include a live map display (GPS location), a 'friendly drones' whitelist to support the operation of pre-approved drones, a 'neutralize on the ground'

feature and an average detection and takeover duration of 10 seconds.

Find out more at www.convexum.com

Signyfy - The Future of Light

Signyfy's energy-efficient LED lighting and smart lighting control minimizes lighting energy usage and helps you achieve your sustainability goals. The Interact IoT Platform enables connected LED lighting systems and embedded sensor networks to collect data and deliver insights, benefits and new services by interacting with Security Systems.

Broadband data through light is a massive support to security systems and operations. In 2018, Signify became the first global lighting company to LiFi-enable normal office lighting fixtures. Their technology provides a fast, stable broadband connection through light waves and, they say, is ideal in areas where WiFi cannot be used or where there's poor or no wireless connection. This makes it a great support for Access Control and Intruder Alarm Systems as well as for CCTV.

See more information at www.signyfy.com

RFID technology for turnstiles

Physical security personnel cannot always track the arrival of every person, which means some individuals might enter buildings or use elevators to access areas that are off-limits.

As part of its solution, Essex Electronics is building HID Global's RFID-based technology into its new iRox-T turnstile reader. HID Global has already provided its 13.56 MHz HF RFID readers for use at access-control beyond doors, at gates, including turnstiles, but now, the system will provide a seamless RFID-enabled turnstile as part of HID's "Connected Building"

strategy. The turnstile-based technology is one part in HID's long-term plan to offer a Connected Building approach for use by office workers and visitors to manage access areas such as parking lots, front doors and elevators.

More information can be found at www.keyless.com or www.hidglobal.com

Axis - License Plate Recognition

Axis Communications has released a camera specially designed to capture clear and sharp license plate images from vehicles moving at speeds of up to 130 km/h (81 mph). The AXIS Q1700-LE License Plate Camera ensures the required pixel density for license plate identification in one lane traffic at a range of up to 100m during daytime and up to 50m at night. It's compatible with AXIS Camera Station and can be used with server-based or edge analytics from most third-party vendors to perform further analysis of recorded or live material.

Go to www.axis.com



Please note that none of the items covered in this section are endorsed by TAPA.

OVER 30,000 REASONS TO USE TAPA'S INCIDENT INFORMATION SERVICE INTELLIGENCE DATABASE

To see favourites here, select 'F' then 'S', and drag to the Favourites Bar folder. Or import from another browser. Import favourites

TAPA
Transported Asset Protection Association

IIS Database / Secure Parking

Filter Parking Spots
From: 12/04/2019 To: 12/07/2019
Incident Category: Ignore filter
Modus Operandi: Ignore filter
Location Type: Ignore filter
Country: France
Region: Ignore filter
Product Category: Ignore filter
Route Planning
Apply filter and refresh list
Reset filter
Download selected incidents (CSV)
Download selected parking spots (CSV)
Report an incident

List Map Archive
Incidents Parking Spots
Full Screen Toggle Heatmap

When planning secure transport routes, TAPA members benefit from access to the Incident Information Service (IIS) database, which highlights recorded incidents and helps to determine areas to avoid to keep supply chains resilient.

Clearly, some routes are safer than others – but where are the worst cargo crime ‘hotspots’ and how do you avoid them? If you can’t do so, can you identify secure parking sites along your intended route for drivers’ rest breaks? when drivers need to take rest breaks?

These are just some of the questions TAPA members can help to answer by using the Association’s Incident Information Service (IIS) intelligence database. It holds information on over 30,000 cargo crimes globally and adds hundreds of new incident reports on freight thefts every month.

Quick and easy to use, TAPA's IIS enables you to see:

- The date of each incident
- Type of incident, i.e. Theft from Vehicle
- Modus operandi used by the offenders
- A description of the incident, where available
- The type of products stolen
- Value of the loss if financial data has been reported
- The location of the crime, i.e. Origin Facility
- The town, district, region and country where the crime occurred
- GPS coordinates of recorded cargo losses
- A mapping tool to identify secure parking sites for future route planning

To make using the service more user-friendly, this month the Association has introduced new legend icons to make it even easier to identify specific types of cargo crimes on incident maps based on your criteria. Clicking on any of these icons provides information on a cargo crime in this location as well as the option to drill down to see more detailed intelligence.

It has never been easier to share incident intelligence...

The 30,000-plus cargo crime reports in the IIS database have come from a variety of credible sources, including law enforcement agencies, TAPA members, insurers and reputable media outlets. You don’t have to be a victim of a cargo crime to use the service, you can use the IIS tool to upload any incident intelligence you have gained. Or you can send news links you have seen on cargo crimes to TAPA’s IIS team.

If you are a victim of cargo crime, rest assured that IIS will not publish your company name. We simply want to gather as much intelligence as possible into criminal activities to prevent future losses occurring.

Watch our 2-minute Explainer Video and learn how easy it is to send a report to IIS or to use the service as part of your own supply chain resilience programme.

WATCH NOW

Our new IIS Incident icons



Level 1



Level 2



Level 3



Partner



Theft from Facility



Theft of Container



Theft of Vehicle



Theft from Train



Theft from Container



Theft from Trailer



Theft from Vehicle



Theft of Trailer



Truck Theft



Fraud



Clandestine



Hijacking



Theft



Robbery



Multiple Incidents



Unknown

THE INSIDE JOB

As the volume of cargo crimes reported to TAPA's Incident Information Service (IIS) increases and intelligence originates from more countries globally, various trends are being highlighted, such as the number of losses involving an 'Internal' modus operandi. The classic 'inside job' is a challenge for every company and particularly those where employees have regular access to high value, theft targeted goods. Of course, it's only a very small minority of staff who are tempted to break the law but the impact of subsequent losses can be far-reaching. The recently-published BSI and TT Club *Cargo Theft Annual Report 2018* offers more insight – and some sound advice – on how to deal with what it describes as a 'common vulnerability'...

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

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

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

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

The most frequent types of insider activity identified were unauthorised disclosure of sensitive information (47%) and process corruption (42%). Noteworthy demographic information from the study indicated that significantly more males engaged in insider activity (82%) than females (18%) and 49% of insider cases occurred within the 31-45 years age category.

The study also revealed:

- Most insider acts were carried out by permanent staff (88%); while only 7% of cases involved contractors and 5% involved agency or temporary staff
- The duration of the insider activity ranged from less than six months (41%) to more than 5 years (11%)

- More than half of the cases were identified within the first year
- 60% of cases were individuals who had worked for their organisation for less than 5 years
- Most insider cases in the study were self-initiated (76%) rather than as a result of deliberate infiltration (6%); i.e. the individual saw an opportunity to exploit their access once they were employed rather than seeking employment with the intention of committing an insider act.

Financial gain was the single most common primary motivation (47%) and most closely linked to process corruption or giving access to assets.

Recruiting and ongoing managing of staff

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

Pre-employment screening seeks to verify the credentials of job applicants and to check that they meet preconditions of employment. When conducting checks, it should be established whether the applicant has concealed important information or otherwise misrepresented themselves. To this extent, pre-employment screening may be considered a test of character. The ways in which pre-employment screening is performed vary greatly between organisations.

€165,000+

The average loss for cargo thefts with a value stating an 'Internal' modus operandi





'An insider could be a full-time or part-time employee, a contractor or even a business partner. An insider could deliberately seek to join an organisation to conduct an insider act or may be triggered to act at some point during their employment.'

79

Cargo thefts with an 'Internal' M.O.
were reported to TAPA globally in the
first six months of 2019



13

The number of major cargo crimes
with a loss value of €100,000 or more in
H1/2019 featuring an 'Internal' M.O.





The aim of pre-employment screening is to obtain information about prospective or existing staff (if promoted and/or changing jobs in the organisation) and use that information to identify individuals who may present security concerns. Pre-employment screening is the foundation of good personnel security. It allows you to confirm the identity and credentials of those you are granting access to your sites and information and reduces the likelihood of an insider harming your business. British Standard 7858 (BS7858) sets out recommendations for the security screening of individuals to be employed in an environment where the security and/or safety of people, services, personal data or property is a requirement of the employing organisation's operations or where such screening is in the public or corporate interest.

Initial screening of personnel is a vital component to any business's security management process. Effective screening satisfies several critical areas including confirmation that the person applying or presenting themselves to undertake a role is both qualified, capable, trustworthy and of good character. It is clearly important to know that the person can undertake the required task, from a competency point of view, however just as important, if not more so, is to ensure from a security perspective you are able to verify that they are who they say they are. Many identity documents can easily be

fraudulently doctored, and operators should develop a process which allows for only a small number of key official identity documents to be used, for example a current drivers' licence and a passport, that can be verified quickly and confidently through official channels.

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

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

23

Number of countries worldwide reporting 'Internal' cargo crimes to TAPA's IIS in the opening six months of 2019



Ongoing personnel screening

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

Regular performance reviews should be undertaken. Whilst performance can obviously be more closely managed, it may be that a change in personal circumstances may be identified through a process such as but not limited to; a change of relationship status, change of address, change in financial circumstances, or a change in their ability to perform their role, such as having their driving licence revoked.

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

€3.4m

Highest value individual losses with an 'Internal' M.O. in the first six months of 2019; the loss of a shipment of agricultural materials by a bogus freight forwarder using falsified documents on 9 February and the theft of a cash-in-transit vehicle in Aubervilliers, France, on 11 February



Whilst our primary focus in this report is the risk of cargo theft, the identified principles should serve to highlight wider associated risks concerned with the theft of vehicles, trailers, chassis, containers, other CTUs, identity and fuel. Where mobile personnel are concerned, in practice you are allowing them full trusted access to:

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

Temporary staff

In any business there will inevitably be periods of peak demand where temporary personnel are required and often at short notice. These occasions are ones where the diligent operator must have robust processes in place. Commercial and operational time pressures should not supersede the need to perform full due diligence checks, specifically



checking to see if their employment has ever been terminated by a previous employer to understand the reasons why.

Where an employment agency is used, ensure that you fully understand and are satisfied with their due diligence procedures. What are they checking and how? Are they able to satisfy some of your requirements prior to the temporary worker arriving at your site? What are the terms and conditions of the employment agency? Do they provide any liability cover if one of their temporary workers is either not capable of undertaking the task they are required to or causes loss through an act of negligence?

Management controls

Clearly there exist specific critical areas of focus around recruitment where mitigation of this type of risk is concerned. Notwithstanding these, more general management controls

also need to be considered. The risk emanating from everyday operational procedures may not be immediately identifiable; however, each breach of such management controls should be considered a near miss and could serve to weaken the entire security management program. Whilst not an exhaustive list, some of the key controls and considerations are:

- **Do your employees have access to your customers' premises, systems or data?** To what extent is access required and granted and on what basis? Does your customer have security requirements, are you able to adhere, manage and control these requirements for the personnel deployed?
- **Access to company uniform** – it is often preferable to have both permanent and temporary personnel in company uniform. From a brand recognition and customer satisfaction perspective this can certainly be beneficial. Due consideration, however, should be given to control of the distribution of uniform. Could a temporary worker use the uniform to mis-represent themselves or others, posing as an employee of yours, allowing them access to premises, vehicles or cargo?
- **Access to ID badges** - Identification badges are implemented as a means of security control. Badges can allow access to restricted areas. Strict controls need to be considered to monitor and manage the distribution of such badges. Are people able to use each other's badges? Do temporary personnel require a full access badge, or can their access be restricted?

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



14

In the first half of 2019, TAPA's IIS recorded losses in 14 separate product categories with an 'Internal' M.O.





Social Media and general communications

Social media is becoming an increasing, albeit less obvious, security threat. Especially amongst lone working mobile personnel, social media is frequently used as a means of keeping in touch with friends, family and colleagues. All posts, however, are location sensitive and therefore traceable and have the potential to divulge a series of valuable security data to organised criminals. Including the time, date and location, it can also - for example - illustrate that the driver is away from their vehicle.

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

Whilst it may be challenging to restrict personnel from using social media platforms to communicate, operators should consider

39.2%

31 of the 79 losses reported to the Association between 1 January-30 June 2019 occurred when transport vehicles carrying the goods were en route



26.5%

Russia was the country with most 'Internal' freight theft incidents in the first half of 2019, with 21 or 26.5% of all such reported crimes



providing awareness training outlining the risks of the information being shared and how it might be used in the wrong hands.

More traditional methods of communication should also not be forgotten in this regard. Awareness training of all personnel should consider the risks of unwittingly divulging what could be valuable information to strangers.

Conversations with peers about the cargo you are handling or carrying at any given time, or perhaps a regular collection from a certain site or delays experienced at a certain site can all be valuable to the organised criminal. You don't know who might be listening to your conversation!

SECURITY

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

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

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

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

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

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

To read the full report and its recommendations, [click here](#)



TAPA SECURITY STANDARDS ARE PUTTING RESILIENT SUPPLY CHAIN SERVICE PROVIDERS ON THE MAP ACROSS EMEA

The number of TAPA Security Standards certifications in the Europe, Middle East & Africa (EMEA) region climbed to another new 22-year high in the first half of 2019 as the Association continued to see more take-up of its Facility Security Requirements (FSR), Trucking Security Requirements (TSR) and Parking Security Requirements (PSR).

Companies looking to work with TAPA FSR certified sites now have a choice of 699 facilities in 61 countries in EMEA as 47 more certifications were awarded in the second quarter of 2019, up 7.2% year-on-year.

The top five countries in the region for FSR certified facilities are now:

- United Kingdom – 96 certifications
- Germany – 56
- Italy – 49
- Netherlands – 87
- Spain – 46

Other countries with 10 or more FSR facilities are:

- Sweden - 29
- United Arab Emirates - 29
- France - 23
- Turkey - 23
- Czech Republic - 20
- Poland - 19
- South Africa - 18
- Belgium - 16
- Ireland - 16
- Russia - 15
- Austria - 14
- Hungary - 14

It's a similar story for TSR and PSR. With more transport and logistics companies and their customers looking to ensure the security of their goods during transportation, another 29 operators established TSR-certified fleets in Q2/19. There are now 170 trucking providers in 29 countries in EMEA with TSR certifications, an increase of 20.5% over the same period a year ago, with 46 of these in the Netherlands, 18 in Italy, 13 in Germany, nine in both Romania and the United Kingdom, and eight in Belgium and Poland.



The number of Parking Place Operators joining TAPA's secure parking programme rose 136.8% versus a year ago. The 45 sites currently visible in the Association's online database provide more than 4,500 parking places in 10 countries.



Thorsten Neumann, President & CEO of TAPA EMEA, is confident the current record will be broken again in the second half of the year. "Our focus is to help our members deliver a resilient end-to-end supply chain and our Security Standards – which

have been developed by the industry – give companies not only the procedures and processes they need to manage risk, they also come with the TAPA stamp of integrity. We will continue to look for more ways to help companies with FSR, TSR and PSR certifications gain value from their commitment to the highest levels of supply chain security."



THE ESSENTIAL ROLE OF MANNED GUARDING IN THE DEVELOPMENT OF THE MALAYSIAN SILK ROAD

Tony Lugg, Chairman of TAPA APAC looks at how the region's Guarding Security Requirements (GSR) will help to address the newest risks and challenges in the supply chain connecting China with South East Asia as well as Europe as the 'Belt and Road' initiatives go full steam ahead.

The question often raised is what is TAPA doing to secure these emerging supply chains? Well, for over 20 years, TAPA has helped Manufacturers, Logistics Service Providers, Security Service Providers (SSP) and other supply chain stakeholders, including Government & Customs (AEO, C-TPAT, STP) agencies and Law Enforcement, to risk manage



and build resilient supply chains. As the supply chain constantly reinvents itself, the challenge for industries is to gear up to meet the new challenges before them. This means the security industry has to adapt or risk falling behind.

The recent six-day trade and investment mission to the US co-organised by the

Malaysian Investment Development Authority, Malaysia External Trade Development Corp and InvestKL Corp, is projected to have generated some RM6.6 billion in potential investments in Malaysia for the manufacturing, services and other industry sectors. And, this month, Bloomberg reported that China has struck a deal with Malaysia to resume the East Coast Rail Link project, which is regarded as a boom for China's 'Belt and Road' initiative.

From a security perspective, in response to such initiatives and challenges, one of TAPA APAC's objectives is to further integrate security partners into supply chain processes, including the standardization of Guarding Services across the Asia Pacific region for logistics sites. Borne out of this strategy came the TAPA Guarding Security Requirements (GSR), a regional Security Standard for APAC. As with the consistency across facilities and trucking operations offered by TAPA's global Security Standards, members with TAPA certified facilities in APAC felt that the level of guarding services that they procure should be the same at all of their sites, irrespective of whether they are in Indonesia, Thailand, Philippines, Malaysia or elsewhere in the region.

This month, Bloomberg reported that China has struck a deal with Malaysia to resume the East Coast Rail Link project, which is regarded as a boom for China's 'Belt and Road' initiative.



Previously, there was no measurement or standard in place to create alignment and a regional standardization of process. Members observed that security services providers employed in securing TAPA certified sites, although providing good service, often misunderstood the TAPA philosophy and requirements, which created a gap. That gap equated to risk and exposure and, on occasions, had contributed to security failures. In some examples, insider collusion had taken place resulting in major losses from sites.

Research showed that guarding companies manning TAPA certified sites, were (1) generally unaware of TAPA's requirements, or (2) had difficulty in understanding the requirements. This was apparent especially where the SSP was responsible for meeting TAPA's requirements for Access Control Management, Perimeter Security, Guard House Duties, CCTV and Alarm Monitoring. It was apparent that the TAPA Standards did not read across into Guarding SOPs and visa-versa. The TAPA Guarding Security Standard was developed by TAPA APAC to create alignment.

The introduction of GSR means that members can have one regional standard and benchmark in place to protect and measure each site. With more manufacturing companies looking to Malaysia as an alternative to China due to rising labour costs, it means that the supply chain and security industry needs to step up and develop a seamless integration of people, processes and systems as Malaysia's connectivity continues to grow. According to the DHL Global Connectedness Index (GCI) report, Malaysia has maintained its strong position globally, ranking second highest in Southeast Asia and 12th out of 169 countries for trade connectivity.

TAPA is responding to the needs of its members and helping to develop the resilience and sustainability of these new networks. Cross-border security is a key to success and, as an enabler for trade facilitation, TAPA offers experience in securing cross-border supply chains around the world, especially the Asia Road Network spanning some 3000kms from China, Vietnam, Laos, Cambodia, Thailand, Malaysia and Singapore, where several Logistics Service Providers have achieved TAPA's

'With more manufacturing companies looking to Malaysia as an alternative to China, the introduction of GSR means that members can have one regional standard in place to protect and measure each site.'

Level 1 certification for its Trucking Security Requirements (TSR) to meet the growing demand for ground services.

The GSR offers a solution for Buyers to integrate their security and safety protocols between Security Service Provider (SSP) and guarding security companies' service standards, providing advantages such as:

- Acting as a written service level agreement and adherence of best practices prerequisites between the Buyer, Logistics Service Provider (LSP) and Security Service Provider (SSP)
- Cogent Guarding Standard Operating Procedures (SOPs) with regards to Roles, Responsibilities and Accountabilities
- Established Key Performance Indicators (KPI) regularly reported and reviewed to drive efficiencies
- Ensuring that SSPs only deploy guards who are sufficiently trained and qualified to carry out their duties
- Facilitating a process of continual improvement

The goal of TAPA APAC's GSR Working Group has been to seamlessly integrate the GSR with other TAPA Standards to ensure that all requirements of the Standards are met. Manned Guarding Services companies play a major role in securing supply chains and the GSR pilot will allow us to test all areas and make improvements where required.

Part of the current Silk Road development addresses the rail connectivity between China and Europe as well as future and current rail and road connectivity with South East Asian countries. When the rail connection first started to Europe, it attracted the attention of electronics manufacturers which saw an opportunity to ship fast-moving

consumer goods (FMCG) even faster. The local government also offered incentives to manufacturers in the west of China, including subsidies for rail freight transport.

As the supply chain evolves further, new standards will be required to meet the needs of shippers of high value, theft targeted goods. The next revisions of TAPA's global Security Standards as well as the development of a Supply Chain Cyber Security Standard aim to provide a holistic certification programme to meet manufacturers' needs for 2020 onwards.

Depending on the complexity and size of the supply chain, compliance with TAPA Standards may be achieved through a single LSP/Applicant or multiple LSPs/Applicants and qualified subcontractors. The 'Belt and Road' initiatives aim to boost mutual investment and trade between China and countries along the neighbouring routes, facilitate connectivity between those countries, and support their pursuit of a new type of industrialisation.

The GSR can be referenced in agreements between Buyers, Logistics Service Providers, Guarding Operations and/or other Applicants seeking a TAPA partnership, certification or a Mutual Recognition Agreement based on TAPA GSR. It has currently been rolled out in Malaysia, Singapore and the Philippines and, just recently, Sankyu Logistics PTE LTD became the first company in APAC to certify two of its logistics facilities in Singapore.

This milestone was a great achievement by everyone involved in the development of GSR and, we hope, the first step in its wider adoption in supply chains across the APAC region.

Note: The TAPA GSR Standard is a regional TAPA Standard developed by TAPA APAC to support its members. There are currently no plans for GSR to be adopted globally by the Association.

AMERICAS NEWS



CTPAT, CRIMINAL INVESTIGATIONS BY THE U.S. FOOD & DRUG AGENCY, AND PERSONAL PROTECTION WERE ALL ON THE AGENDA AT TAPA AMERICAS' T1-MEETING



TAPA Americas held its T1-Meeting in Atlanta, Georgia, this year. Hosted by Cisco Systems, the event featured speakers from the U.S. Customs-Trade Partnership Against Terrorism, the U.S. Food and Drug Administration, and the Center for Personal Protection and Safety.

Carlos E. Ochoa, Branch Chief CTPAT Headquarters, provided a look into the new "Minimum Security Criteria (MSC)." The Customs-Trade Partnership Against Terrorism is a voluntary public/private initiative that builds cooperative relationships to strengthen and improve overall international supply chain and U.S. border security. CTPAT is widely recognized as one of the most effective means of providing the highest level of cargo security through close cooperation with international

supply chain businesses such as importers, carriers, consolidators, licensed customs brokers, and manufacturers.

It has been 17 years since new criteria was added to the program. And, while there have been updates to CTPAT since the program was established in 2001, the new MSCs are based on lessons learned over time, and the increase of different types of terrorism. According to Carlos, the reality is that when CTPAT was established, the United States was concerned with Al-Qaeda but, now, the United States is facing ISIS, huge migration waves from Europe and North Africa as well as from South America – and these new security threats require new security criteria with a great emphasis on business partnership.

The new MSC reflects the inclusion of the three new security criteria categories and has left CTPAT members scrambling to figure out what must be done to meet the new criteria and what other actions should they consider

'When CTPAT was established, the United States was concerned with Al-Qaeda but, now, the United States is facing ISIS, huge migration waves from Europe and North Africa as well as from South America.'

to remain validated CTPAT members. The new MSC categories and CBP's recommendations for compliance are: 1) Security Vision and Responsibility 2) Cybersecurity and 3) Agricultural Security. Carlos pointed out that other noteworthy highlights to the MSC are new eligibility requirements, forced labor recommendations for importers and foreign manufacturers, and additional training tools. The official rollout was conducted at the CTPAT Conference in late June.

Ronne Malham, Assistant Special Agent in Charge, Midwest Area/Chicago Field Office, Office of Criminal Investigations, U.S. Food and Drug Administration, provided attendees with an in-depth overview of his department. The criminal side of U.S. Food & Drug Administration, the Office of Criminal Investigations, handles any criminal activity covered under the Food, Drug, and Cosmetic Act (FDCA).

The Midwest Area Office covers the surrounding seven-state region: from the Dakotas through Minnesota and Wisconsin, down through Illinois, and up around Lake Michigan through Indiana and into all of Michigan. All of its Special Agents come with around ten years of experience or more from larger federal agencies such as DEA, HSI, U.S. Postal Inspection Service and U.S. Secret Service, and most of them were local or state police prior to that.

The Office's most typical cases involve "supply chain" interstate criminal activity: imported illegal drugs and devices and illegal foreign unapproved drugs attempting to infiltrate the legitimate supply chain, theft of pharma cargoes, tamperings that rise to a federal level (i.e. tamperings of opioids by hospital, other healthcare practitioners, and fire/rescue personnel that tamper at the patient point of care or prior to that point is the most common), and criminal disruption of FDA's civil inspection process, i.e. false statements or intentional misleading by companies under civil inspection authority. The agency offices are getting more involved with opioids too; usually not the street stuff that DEA or HSI work, so much as when there is an attempt to



AMERICAS NEWS

counterfeit a branded product, i.e., organized groups adding illegal fentanyl and creating pills that are branded to look like oxycodone or hydrocodone. The short answer is: if there is a nexus to FDCA criminal charges, we may be able to work it. Its agents have worked closely with global security teams from corporate and pharma entities with success in addressing criminal activity.

Drew Jenkins, Vice President for Operations, Center for Personal Protection and Safety, gave a presentation addressing the importance of travel safety training to any organization with a travel population. Whether going to Toledo or Tibet, it is vital for the individual traveler to be prepared for the environment they are visiting. The key factors in travel safety boil down to preparation, situational awareness, and being proactive about what the traveler might encounter. Each organization sending people on travel trips, similarly, must be prepared as well with solid plans, directives, and standard operating procedures – the most important of which is having a communications plan with back-ups, he told TAPA Americas' T1 delegates.



Scott Dedic and Bill Rice of TAPA Americas at the Atlanta T1-Meeting.



**WELCOME TO
OUR NEW
MEMBERS**

TAPA AMERICAS BOARD MEMBER WINS LOSS PREVENTION MAGAZINE'S 'EXCELLENCE IN PARTNERSHIPS AND COMMUNITY SERVICE' AWARD



John Tabor, Senior Vice President, National Retail Systems, and a member of TAPA Americas' Board of Directors, has won *Loss Prevention Magazine's* 'Magpie Award' for 'Excellence in Partnerships and Community Service'.

The Awards celebrate industry accomplishments on an ongoing basis, recognizing the loss prevention professionals, teams, solution providers, law enforcement partners, and others that demonstrate a stellar contribution to the profession.

"When building business partnerships, listening and learning are the two most critical pieces," he said. "Whether it's listening to customers' needs, understanding our employer's expectations, or listening to the employees themselves, there's a lot of great talent with wonderful ideas that can lead to substantive change within an organization. Also, ongoing learning is critical. When you think there's nothing more you can learn, that's pretty much career suicide. Not allowing individuals at all levels of the organization to get out and network is probably one of the worst management decisions that a leader can make. It creates a glass ceiling for the employee."

For those working their way up the career ladder, Tabor stresses the importance of communication. "Just about every leadership tool we end up putting in our toolbox is something we've learned from someone else," he said. "Too often today we see people's eyes buried in their cell phones. No one is talking anymore. Having the ability and humility to communicate, understand, and have compassion is essential."

That same compassion and understanding has served Tabor well in his personal life. He has served as a volunteer fireman in his hometown for more than 30 years, acting as a first responder at Ground Zero during the events of 9/11. He also sits on a board working with children born with Down syndrome, recognizing those who make a difference, and providing learning tools that will help them reach their full potential. He assists with autism awareness groups, Homes for Heroes, and cancer-recovery initiatives. Most recently, he was involved in a fundraiser following a fatal New Jersey school bus crash, which took place in his hometown.

"I cannot say enough about the importance of getting involved and supporting your community," John says. "Volunteering can be a life-changing experience. I've always loved giving back, coaching, helping with events, and so forth. Being able to contribute gives me great pride and a sense of fulfillment like nothing else."

Anthony Leimas, Chair of TAPA Americas, said: "We are proud to have John as a member of our Board of Directors. As an Association we rely on volunteers who want to use their expertise to help others and we are grateful for all this support. As this award shows, John goes above and beyond in so many ways and is thoroughly deserving of this honor."

Please join us in welcoming the latest members to join TAPA Americas...

Company	Country	Website
Echo Global Logistics	USA	https://www.echo.com
Logistics Services Panama	Republic of Panama, Central America	http://www.lspty.com
JUSDA Supply Chain Management Services	USA	https://www.jusdausa.com
Kawliga Express LLP	USA	https://www.kawligaexpress.com

EUROPE, MIDDLE EAST & AFRICA REGION

CARGO CRIME MONITOR

CARGO THEFT BY COUNTRY

June 2019

Belgium	4 (3.6%)
France	5 (4.5%)
Germany	8 (7.3%)
Netherlands	51 (46.5%)
Romania	5 (4.5%)
South Africa	8 (7.3%)
Spain	1 (0.9%)
Sweden	1 (0.9%)
Uganda	1 (0.9%)
United Kingdom	22 (20%)
Zimbabwe	4 (3.6%)

Number of incidents in month



€355,892

Average loss for the 7 major cargo crimes reported to TAPA's Incident Information Service (IIS) in June 2019



€2,819,855

Total loss for the 19 or 17.2% of crimes stating a value

15

Number of TAPA IIS product categories recording cargo thefts in June 2019



110

Number of new cargo crimes recorded by TAPA's IIS in EMEA last month

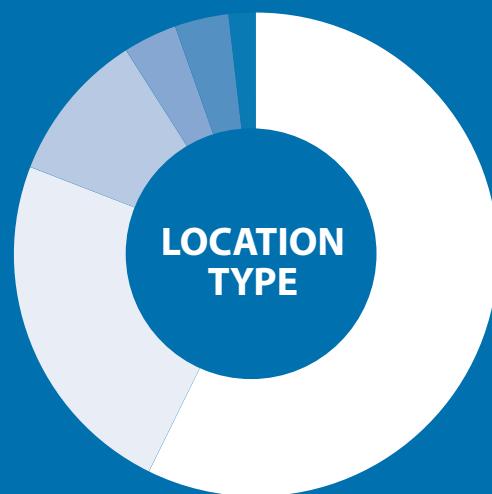
€1,200,000

Biggest single loss -
Theft from Trailer of
miscellaneous
technology products at a
motorway service area in
Kent, UK, on 12 June

Number of countries
in EMEA reporting incidents

11

Theft from Vehicle.....	61 (55.5%)
Theft of Vehicle.....	11 (10.1%)
Theft from Trailer.....	9 (8.1%)
Theft.....	8 (7.3%)
Theft of Trailer.....	7 (6.4%)
Theft from Facility.....	6 (5.4%)
Truck Theft.....	3 (2.7%)
Hijacking.....	3 (2.7%)
Theft from Container.....	1 (0.9%)
Theft of Container.....	1 (0.9%)



2

Crimes in EMEA recording a loss value of between €50,000 & €100,000 produced a combined loss total of €118,280

7 – Number of major incidents with a loss value over €100k

€148,413 AVERAGE LOSS VALUE LAST MONTH

23.6%

Or 26 of the recorded incidents took place in Unclassified Parking Locations



MODUS OPERANDI USED IN LATEST CARGO THEFTS:

Intrusion	49 (44.6%)
Unknown	40 (36.4%)
Violent & Threat with Violence	14 (12.7%)
Forced Stop	3 (2.7%)
Deceptive Stop	3 (2.7%)
Theft from Moving Vehicle	1 (0.9%)

LOSSES FROM SUPPLY CHAINS EXCEED €2.8M IN 30 DAYS AS TAPA RECORDS CARGO THEFTS IN 11 COUNTRIES ACROSS THE EMEA REGION



With cargo losses in the Europe, Middle East and Africa (EMEA) region being added to TAPA's Incident Information Service (IIS) database daily, this report looks at some of the higher profile cargo crimes reported to the Association last month.

The total loss for the 17.2% of all recorded incidents with a value of **€2,819,855** produced an average loss for these thefts from supply chains in June of **€148,413**.

TAPA EMEA received intelligence on seven major thefts with values of more than **€100,000**, including one seven-figure loss in the United Kingdom on 12 June. This Theft from Trailer crime saw the offenders target a truck parked at Clacket Lane motorway service area (MSA) on the M25 in Surrey between 20:30hrs and 05:30hrs. The goods stolen included various technology products; smart watches, cycling computers, satellite navigation systems and boating devices with a reported value of **€1.2 million**. 

Vigilant has been asked not to share information on two of the major losses added to its database last month but the other high value thefts included:

€346,667

On 1 June in Rogat in the Dutch province of Drenthe, thieves climbed a fence to enter the transport yard of an Authorised 3rd Party Facility and drove away a trailer loaded with 20 pallets of taps. 



€300,000

Three days later on 4 June, offenders targeted another Authorised 3rd Party Facility – this time in Neustadt-Bad Windsheim in Bavaria, Germany – and stole a semi-trailer and three tractors. After forcing their way onto the site at night, they drove the trailers to the Eastern border but were apprehended by border control officials.



€111,620

Thieves took a 28-tonne low loader and other items, including a generator, from a layby on the A167 main road in Richmond, North Yorkshire, on 21 June.



€100,000

A truck with a shipment of sound bars was attacked by cargo thieves on the A73 highway in Haps, a village in the Dutch province of North Brabant, on 29 June. This was one of a series of freight thefts on the A73 reported to TAPA's IIS last month. Other crimes included product losses of:



- IT components in Venray, Limburg
- Concentrated juice in Venray
- Coffee makers in Venray
- Fuel in Venray
- Powdered soup in Roermond, Limburg
- Metal in Lekkant, North Brabant
- Plastic gloves in Roermond
- Electrical plugs in Haps
- Car polish in Haps
- Computer/laptop products in Haps
- Bicycles in Venray

In the **€50,000 to €100,000** loss category, the incident with the highest value involved the theft of **€65,000** of microwave ovens from a trailer parked at Beaconsfield MSA on the M40 in Buckinghamshire, United Kingdom, on 6 June.



Based on the June data that had already been recorded as the July issue of *Vigilant* went to press, the Netherlands had recorded the highest number of losses for the month in the IIS database. In addition to the incidents mentioned earlier in this article, other incidents included thefts from supply chains of:

- Alcohol in Duiven, Gelderland
- Copper in Zwolle, Overijssel
- Tyres in Hank, North Brabant
- Car engines in Hoorst aan de Maas, Limburg
- Animal supplies in Liempde, North Brabant
- Vacuum cleaners in Coevorden, Drenthe
- Cigarettes in Deurningen, Overijssel
- Coffee in Lierop, North Brabant
- Perfume in Duiven, Gelderland



In the United Kingdom in June, TAPA EMEA was notified of several attacks by offenders who threatened truck drivers with knives:

- In Renfrewshire, Scotland, targeting cash-in-transit
- A driver held at knifepoint in Sandwell in the West Midlands while his vehicle and unspecified cargo were stolen
- A group of offenders in West Bromwich in the West Midlands – one armed with a knife – who dragged a driver from his cab before stealing the vehicle and its load
- An assault on a driver at a service station in Northamptonshire and the theft of unspecified cargo



Other crimes in the UK included further evidence of thieves targeting vehicles carrying tobacco products when they are stuck in slow moving traffic in city areas. On 25 June, a car pulled in front of a truck travelling on the A406 in London in order to slow the vehicle, enabling thieves in a white transit van to drive close enough to the back of the truck to open its rear doors and steal a large amount of its cargo.

At a motorway services on the A1 in Barton, North Yorkshire, a driver interrupted thieves as they tried to transfer part of his vehicle's load onto another lorry nearby. Although the offenders threatened the driver, he was able to use his truck to block their escape route, forcing the eight suspects to flee on foot.

Police in the UK have also continued to demonstrate their commitment to reducing cargo crime with the arrests of three men after several trucks reported tarpaulin-cutting crimes at Newport Pagnell motorway services in Buckinghamshire. They also arrested three men on 7 June in Staffordshire who were using an HGV with cloned licence plates to transport cargo they had just stolen. Police officers caught up with the truck on the M1 motorway, which resulted in the offenders jumping from the moving vehicle and leaving it to crash into barriers as they tried to run away.

In Germany, products including copper clippings, coffee and tools/building materials were reported stolen. Crimes were recorded in Berg in Bavaria as well as in Dortmund, Duisburg, Düren and Scholven in North Rhine-Westphalia.



More violent crimes took place in South Africa last month, the most severe of which saw a driver shot in the head and his colleague shot in the stomach as they were engaged in a shoot-out with thieves trying to hijack their truck on the N2 in Durban, KwaZulu-Natal. Two innocent bystanders were also shot as offenders in four cars attacked a cash-in-transit vehicle as it made a delivery to an ATM in Soweto, Gauteng province, on 6 June. Shots were also fired at a police officer who interrupted thieves as they ransacked cargo containers at an Origin Facility in Krugersdorp, Gauteng, on 29 June.

Four armed attackers also stole a container full of clothing and a trailer after holding a security guard at gunpoint at an Authorised 3rd Party Facility in Clairwood, KwaZulu-Natal.

Another driver also fell victim to the frequently seen 'blue light' modus operandi in South Africa. After being told to pull over by the driver of a white 4x4 vehicle with blue lights and informed the truck's tailgate lights were not working, the driver was forced into the boot of the vehicle as he exited his cab to investigate. The driver was en route on the N1 in Pretoria at the time of the incident on 22 June.

Elsewhere in EMEA, TAPA's IIS recorded cases of:

- Four cargo crimes in Zimbabwe – all in Harare. Three involved attacks on vehicles carrying tobacco products while they were en route, while the other crime resulted in a loss of food and drink goods from a Destination Facility;
- In Belgium, IIS received reports of thefts of cosmetics and hygiene products on the E42 in Liege, tobacco products in Rumst, chewing gum in Mons, and furniture/household appliances in Mechelen;



- A Deceptive Stop in France on 25 June resulted in a theft of a vehicle and its unspecified cargo valued at 'tens of thousands of Euros'. The truck was travelling on the A43 between Vaulx and Milieu when it was stopped by a car with a blue light. After ordering the driver out of his cab, one of the suspects climbed into the truck and drove off;
- The use of a door alarm system prevented thieves from stealing a shipment of pharmaceuticals after they broke into a secured compound in Barcelona, Spain;
- In Sweden, offenders escaped with 30 49-inch televisions after slashing the tarpaulin curtain of a truck in Hammarvagen, Gothenburg.



Goods were recorded stolen in 15 TAPA IIS product categories. The top three were:

- Furniture/Household Appliances – 11 losses
- No Load (Theft of truck and/or trailer) – 10
- Tobacco – 10

To see the very latest cargo crime data, TAPA EMEA members are advised to visit the password-protected online IIS database.

Or to report a cargo crime, contact iis@tapaemea.org

PRODUCT CATEGORY	No	%
Unspecified	29	26.4%
Miscellaneous	18	16.4%
Furniture/Household Appliances	11	10.1%
No Load (Theft of truck and/or trailer)	10	9.1%
Tobacco	10	9.1%
Food & Drink	7	6.4%
Computers/Laptops	4	3.6%
Clothing & Footwear	4	3.6%
Car Parts	4	3.6%
Metal	3	2.7%
Cosmetics & Hygiene	2	1.8%
Cash	2	1.8%
Tyres	2	1.8%
Toys/Games	1	0.9%
Tools/Building Materials	1	0.9%
Pharmaceuticals	1	0.9%
Bicycles	1	0.9%



ASIA PACIFIC IIS NEWS



Incidents recorded in India, Bangladesh and the Philippines

Six incidents added to TAPA's IIS database in June in the Asia Pacific region involved:

- On 22 June, TAPA APAC was notified of a forced stop of a 10-wheeler truck by three gunmen, who used their pick-up vehicle to block the road in Samar in central Philippines. They ordered the driver and his helper out of the vehicle before taking over the truck and speeding off towards Tacloban City. The loss value of the unspecified stolen cargo was US\$38,867.

- A similar roadblock M.O. was used by cargo thieves on 16 June to stop a truck carrying electronics products in Bhiwandi, north-east of Mumbai in India. After hijacking the vehicle, they drove it to a secluded spot and stole goods valued at more than US\$14,500 before fleeing, leaving the driver tied up in the truck.
- An 'Internal' M.O. was recorded for the theft of a vehicle carrying a shipment of processed tea in Golaghat in India. According to the incident report on 17 June, the driver was en route when he changed course and started heading towards Dimapur, the largest city in Nagaland. The owner, who had lost contact with his driver, noticed the diversion using the GPS device fitted in his truck and alerted the police, who successfully recovered the vehicle while it was approaching the last police check post at Khatkhati. Police arrested the driver and his helper.



- On 20 June, another violent Theft of Vehicle and its cargo of metal in Brahmanbaria, Assam in India, was reported to TAPA APAC. The driver had stopped at a roadside dhaba when he was overpowered by several attackers and tied up.

The offenders stole the truck and its cargo. Police later found the empty vehicle on the Laluk-Bihpuria road.



- A truck carrying 700 sacks of rice was taken to a warehouse in Sylhet, Bangladesh, on 23 June but instead of being unloaded was held at a refuelling station nearby. When the driver's assistant went to collect the vehicle, he discovered it had been stolen.

- On 24 June in Jharkhand, India, a truck driver parked his vehicle after refuelling and left his assistant to supervise it. On returning, both the truck and the assistant had disappeared along with the unspecified cargo onboard.

STEP UP & STAND OUT

TAPA'S LATEST FSR & TSR SECURITY CERTIFICATIONS

In each issue of this newsletter, we publish a list of the TAPA members that have most recently gained TAPA Supply Chain Security Standards certifications.

The following companies and locations were audited by one of TAPA's approved Independent Audit Bodies (IABs) or, in the case of Class 'C' or Level 3 certifications, may have been completed by an in-house TAPA-trained person.

EUROPE, MIDDLE EAST & AFRICA REGION

FSR	Company Name	Country	City	Class
FSR	Alha-Air Lines Handling Agents S.p.a.	IT	Lonate Pozzolo	A
FSR	Alha-Air Lines Handling Agents S.p.a.	IT	Fiumicino	A
FSR	Alha-Air Lines Handling Agents S.p.a.	IT	Milan	A
FSR	Alha-Air Lines Handling Agents S.p.a.	IT	Prato	A
FSR	DHL Express Germany GmbH	DE	Kassel	C
FSR	DHL Freight Germany GmbH	DE	Duisburg	C
FSR	DHL International UK Ltd	GB	Telford	A
FSR	DHL International UK Ltd	GB	London	A
FSR	DHL Supply Chain	IE	Dublin	A
FSR	Geodis CL	IT	Castel San Giovanni	C
FSR	Itella Logistics OÜ	EE	Rae Vald	A
FSR	Kuehne + Nagel Ltd	GB	Derby	A
FSR	PRL Logistics	IE	Dublin	C
FSR	SC Johnson	EG	Cairo	C
TSR	Company Name	Country	Category	
TSR	Alha-Air Lines Handling Agents S.p.a.	IT	Level 1 / Category Small	
TSR	Transdanubia Speditionsges.m.g.H	AT	Level 3 / Category Small	



ASIA PACIFIC REGION

FSR	Company Name	Country	City	Class
FSR	DHL Express (Malaysia) Sdn Bhd	Malaysia	Kuala Lumpur	A
FSR	Instakart Services Pvt Ltd. (Instakart Rasayani)	India	Rasayani	A
FSR	Tes-Amm (Singapore) Pte Ltd	Singapore	Singapore	A
FSR	Schenker Australia Pty Ltd. (Formerly known as DB Schenker, Perth)	Australia	Perth	A
FSR	Schenker Australia Pty Ltd. (Formerly known as DB Schenker)	Australia	NSW	A
FSR	DHL Korea Ltd	Korea	Seoul	A
FSR	CTS International Logistics Corporation Limited.	China	Shanghai	A
FSR	DHL - Sinotrans International Air Courier Ltd. (PEK South Branch)	China	Beijing	A
FSR	Shenzhen YH Global Supply Chain Co., Ltd.	China	Shenzhen	A
FSR	Hikari International Logistics Limited	Hong Kong	New Territories	A
FSR	Taiwan Air Cargo Terminal Ltd.	Taiwan	Taoyuan	C
FSR	Hong Kong Air Logistics Company Limited	Hong Kong	New Territories	C
FSR	Dimerco Air Forwarders (HK) Ltd	Hong Kong	New Territories	C
FSR	COPE Sensitive Freight Australia	Australia	Canberra	C
FSR	Jentec Storage Incorporated - Iloilo	Philippines	Iloilo	C
FSR	Jentec Storage Incorporated - Davao	Philippines	Davao	C
FSR	Royale Cold Storage Inc - Taytay	Philippines	TayTay	C
FSR	Worldgate Express Services Sdn. Bhd.	Malaysia	Penang	C
FSR	Jentec Storage Incorporated (Bacolod City)	Philippines	Bacolod	C
FSR	Jentec Storage Incorporated (Cagayan De Oro)	Philippines	Cagayan De Oro	C
TSR	Company Name	Country	City	Class
TSR	Circle Logistics Co.,Ltd.	China	Chongqing	Level1
TSR	Ying Wah Transportation Company Limited	Hong Kong	CLK	Level 2
TSR	Shanghai Huasong Logistics Co., Ltd.	China	Guangdong	Level 2
TSR	Mega Union Logistics Limited	China	Shenzhen	Level 2



AMERICAS REGION

FSR	Company Name	Country	City	Class
FSR	Bollore Logistics	USA	Miami	C

STANDARDS FAQs #23



A monthly update by Mark Gruentjes, TAPA EMEA Standards Lead

After receiving a steady stream of questions about TAPA's Security Standards from Audit Bodies and our members, we feel it will be beneficial to share some of the questions received and the responses given by the TAPA EMEA Standards Team. We aim to cover 3-5 questions in *Vigilant* each month.

In this article, we continue to provide you with information on the schedule and changes to TAPA's Security Standards that you will see deployed in the updated 2020 versions. This time, we address multiple questions from the same source as the company holding TAPA certifications is seeking information as it begins to prepare for the updated FSR and TSR Standards.

If you would like to raise a new topic for discussion or ask questions about one of our published responses, please contact us at info@tapaemea.org.



My company has 4 certifications for FSR 2017 and 1 certification for TSR 2017 versions. The recertifications are due between August and December 2020.

Question 1.

I see from previous updates that FSR will be available in single site (as today) or multi-site options. If I were to consider converting my existing 4 certified sites to the single multi-site certification options, what are the main differences, and would I save on auditing costs?

Answer: The physical requirements for single site and multi-site certifications are identical. The differences are with the auditing methods. The FSR multi-site certification option is designed to support operators of 3 or more sites. Additional sites can be added or deleted at any time. Sites will no longer require auditing every 3 years but will be inspected by an audit body on a sampling basis, resulting in less overall audit body visits to the sites. The audit body will be required to inspect the headquarters operation annually. Therefore, the more sites which are added using the multi-site certification option, the greater the potential for savings on audit fees.



Question 2.

I have 3 uncertified sites that I would like to be self-certified to FSR Level C. Can I add these to the multi-site option certification?

Answer: It will not be possible to add self-certified sites to a multi-site certification. Self-certification audits are completed by a representative of the LSP, while multi-site certification audits are completed by an accredited Independent Audit Body. Self-certification will continue to be available under the single site certification model.

Question 3.

I'd like to see the updated 2020 Standards as soon as possible so I can assess any changes I may need to make to my operations. When will they be available for review?

Answer: The FSR and TSR 2020 Standards are going through the final changes. The next draft version will be available in September 2019 and will be available for download by TAPA members. Members will be able to submit comments to be considered by the TAPA World Wide Change Control Board.



STANDARDS SUPPORT



Question 4.

As I make preparation plans for FSR and TSR 2020, will TAPA be available to help me make decisions on the best way to transition to the new versions?

Answer: Yes, and we will welcome these requests. TAPA is a members' association and we want you to gain maximum benefit from your membership.



Question 5.

I am told TSR 2020 will have major changes. Can you assure me that I won't have to make major investments in my truck fleet to maintain my certification status?

Answer: As stated previously, TAPA strives to minimise any additional investment in new systems or technologies but cannot guarantee that costs will not be incurred. TSR 2020 will be reformatted so 4 different transportation modes will now be available and replacing the single "one size fits all" approach. The changes from the existing Security Standards to the new revision are minimal and reflect the opportunity to address unique security measures, e.g. the requirement for a bulkhead between the cab and the cargo space for a van. The major changes will be in new sections that are optional enhancements, a kind of TSR+. These measures can be added to a new or existing certificate to reflect a step up in security from the TSR 1, 2 or 3 levels.

DUBLIN 2019

TAPA EMEA CONFERENCE

23&24 OCTOBER

TAPA
Transported Asset Protection Association

REGISTRATION NOW OPEN



meet THE BOARD

As Vigilant extends its reach to the global TAPA Family, we'll be introducing you to some of the TAPA Board Members in the AMERICAS, ASIA PACIFIC and EMEA regions who are volunteering their time and expertise to drive forward the Association's goal of minimizing cargo losses ... so please meet ...

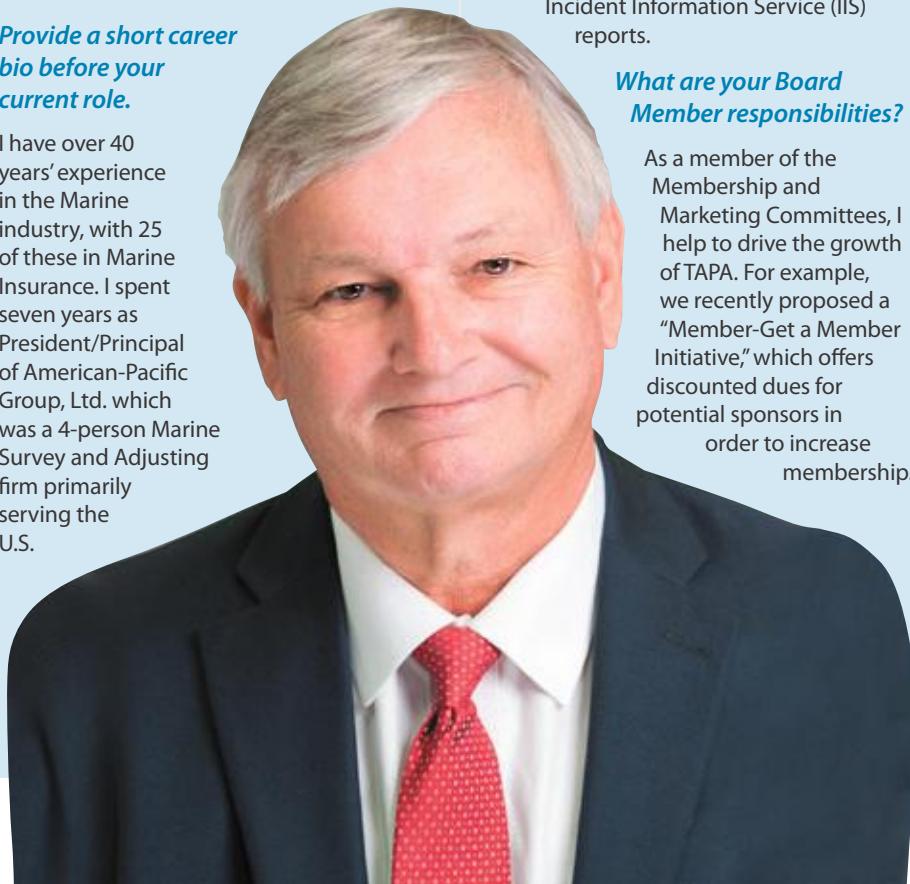
James Neville, TAPA Americas

Introduce us to your day job, title, responsibilities.

I am the Assistant Vice President for AIG's Marine Loss Control Engineering team. In this role I am responsible for helping insureds with marine -related exposure such as cargo; hull and machinery; marine liability; and inland marine develop and execute risk improvement plans that help to predict and prevent loss. I have been in this role at AIG since 2006 and joined the Board in the fall of 2018.

Provide a short career bio before your current role.

I have over 40 years' experience in the Marine industry, with 25 of these in Marine Insurance. I spent seven years as President/Principal of American-Pacific Group, Ltd. which was a 4-person Marine Survey and Adjusting firm primarily serving the U.S.



West Coast, selling my firm to a competitor in 2006 in order to join AIG. Prior to starting my own firm, I spent 5 Years with CNA/Hull and Cargo Surveyors, Inc., San Francisco, CA, which was a nationwide Marine Survey firm. During this position, I gained my early experience in Cargo Theft investigations and Cargo Theft prevention. I have over 13 years sailing time as a Merchant Marine Engineering Officer and, prior to that, spent six years in the U.S. Navy, primarily in the nuclear Submarine Force.

Why was it important to you to become more actively involved in TAPA at the Board of Directors level?

I believe that my Insurance/loss control industry background brings a unique and critical perspective to the TAPA Board of Directors (BOD), particularly as it pertains to Standards, as well as to improving the Incident Information Service (IIS) reports.

What are your Board Member responsibilities?

As a member of the Membership and Marketing Committees, I help to drive the growth of TAPA. For example, we recently proposed a "Member-Get a Member Initiative," which offers discounted dues for potential sponsors in order to increase membership.

What do you bring to your TAPA role?

My deep understanding of the importance of insurance and loss control blends well with our membership's perspectives being in the manufacturing and transportation sectors.

How do you believe TAPA is seen by other supply chain security stakeholders?

I believe that TAPA is very well-regarded by the various stakeholders, and is gaining a larger following in the local, state, and federal law enforcement community that is involved in Cargo Theft Investigation. The annual TAPA Law Enforcement meeting, typically held in December of each year, is consistently growing in attendance.

What are you hoping TAPA can achieve in your region in the next two years – where should its priorities lie?

I believe that the priorities should be in growing the TAPA membership base across all industries, and in promoting the TAPA Standards and programs, particularly the TAPA Level C and 3 Self-Certification programs. I believe that many of the companies that originally self-certify will eventually seek higher levels of full certification.

What are you doing to help attract new members and promote TAPA's Security Standards?

When I engage with companies that are not currently TAPA certified, I talk with them about some of the ways that they can benefit from joining TAPA, such as the conferences, networking opportunities, serving on Working Groups, training, and access to the Incident Information Service (IIS) reports.

How can TAPA gain more cargo crime intelligence in your region?

This is where TAPA's partnership with Federal, State, and Local law enforcement (LEO) is invaluable. These LEO's are on the front line of cargo theft and are among the first to see new Modus Operandi by the criminal element, and to spread the word to other TAPA members on what trends they are seeing. The LEO network also provides for quick response to a theft incident as most have provided their personal cell phones for 24/7 contact for issues in their respective jurisdictions.

If you can change one thing to benefit TAPA Americas and its members during your current term of office, what will that be?

The primary reason that I joined the Membership and Marketing Committees is my interest in growing the membership base. There are many organizations out there that could benefit from the TAPA Standards, yet many of those organizations are completely unaware of our existence. We need to get the TAPA brand out there to all sectors of the supply chain via trade show participation, closer collaboration with related organizations, targeted advertising/articles in the various trade publications, and Member to Member recruitment.

STOP PRESS:



ARMED GANG STEAL \$30 MILLION OF PRECIOUS METALS IN SAO PAULO

As Vigilant goes to press, TAPA's IIS has been notified on a \$30 million theft of gold and other precious metals after thieves targeted a cargo terminal at Sao Paulo-Guarulhos International Airport.

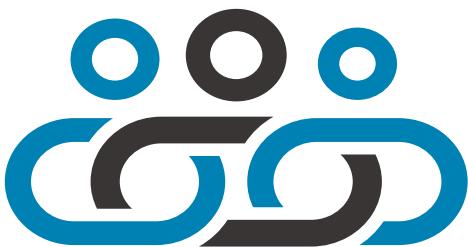


According to reports, the offenders were driving two trucks that resembled those used by the Brazilian federal police.

Ironically, the theft comes in the same month as new data which showed a 38% reduction in cargo crimes in Brazil in the first quarter of 2019.

In the next issue, *Vigilant* will speak to contacts on the ground in Brazil to learn more about the latest cargo crime trends across the country.

WELCOME TO OUR NEW MEMBERS



Please join us in welcoming the latest members to join TAPA EMEA...

Company	Country	Website
Transdanubia Speditionsges.m.b.H	AT	www.transdanubia.com
Protect Vehicle Security	PL	www.protect-vehicle.eu
Levi Strauss & Co.	PL	www.levi.com
SC Smart Autohof SRL	RO	www.smart-autohof.ro
Autopromsnab-spedition LLC	BY	www.aps-solver.com

Please join us in welcoming the latest members to join TAPA Asia Pacific...

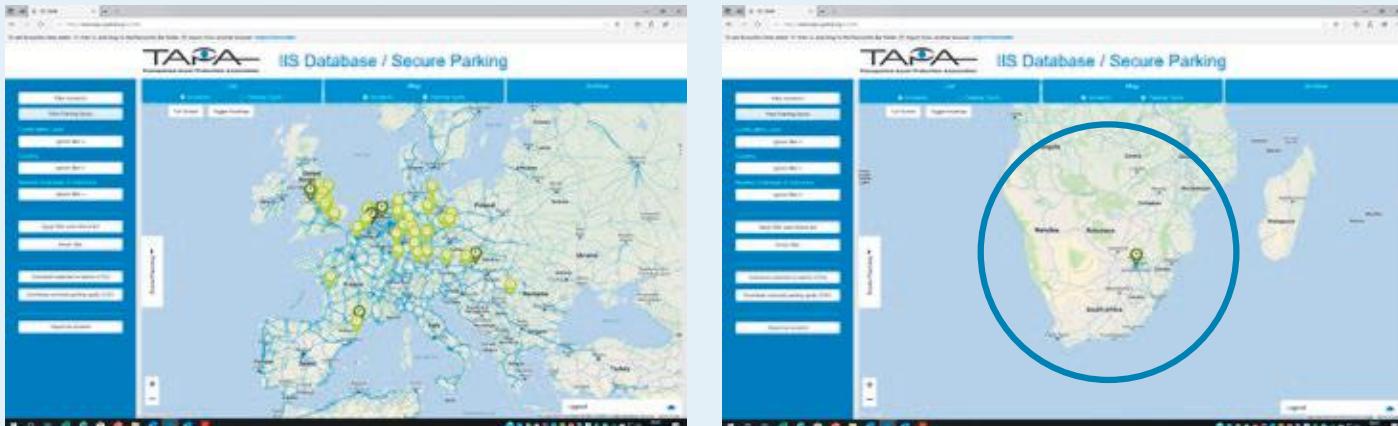
Company	Country	Website
LUG International Trading & Transport WLL	Qatar	https://www.qataronlinedirectory.com/company-details/20200/Lug-International-Trading-&-Transport-WLL
Zuellig Pharma Specialty Solutions Group Pte Ltd	Singapore	https://www.zuelligpharma.com/
Zuellig Pharma Holding	Singapore	https://www.zuelligpharma.com/
Zuellig Pharma Taiwan	Taiwan	https://www.zuelligpharma.com/
Zuellig Pharma Sdn Bhd	Malaysia	https://www.zuelligpharma.com/
港鹏信达物流有限公司	China	N/A
LF Logistics Services Pte Ltd	Singapore	https://www.lflogistics.com/locations/10
Shanghai Time Rider International Transportation Co., Ltd	China	http://en.timerider.com.cn/
IPP Consulting	Australia	https://www.ipp.com.au/

OVER 4,500 SECURE PARKING PLACES... READY FOR YOU



TAPA's new Parking Security Requirements (PSR) and secure parking programme in EMEA is adding new Parking Place Operator sites every month.

You can now use our database to locate secure parking sites in Austria, Belgium, France, Germany, the Netherlands, Romania, Slovakia, South Africa, Spain and the United Kingdom ... and there's much more to come.



PSR PARKING PLACES

