vigilant

THE MONTHLY CARGO CRIME UPDATE FOR TAPA'S GLOBAL FAMILY

CODED WARNING

Ignore the threat of cyber in the new supply chain and you'll be the one taking all the risk

TRANSPORTED ASSET PROTECTION ASSOCIATION

welcome

One global family, one focus, one goal

Welcome to the first global issue of TAPA's *Vigilant* magazine, which is now being circulated to our members in the AMERICAS and ASIA PACIFIC as well as across EMEA.

This is another step in the coming together of the global TAPA Family and, in the months ahead, we will bring you more news and features not only on our respective regions but topics that affect us all.

In this issue we look at what is arguably the biggest threat to our international safety and security; cybercrime. This is not just in relation to supply chain security - it impacts every part of our business and personal lives, and the level of risk is growing day-by-day. Pete Mento, Vice President of Global Trade and Managed Services at Crane Worldwide Logistics, who has addressed TAPA conferences in the AMERICAS and EMEA, gives us a revealing insight into the nature of the threat and why ignoring a problem that is expected to cost $2 trillion a year in 2019 is simply not an option.

Hacking is now both a business and a hobby. We have created an image of a hacker as someone who spends their life in a darkened room, surrounded by technology, but, as Pete highlights, it could just as easily be some seemingly innocent person sat in a coffee shop working away on their laptop. The potential rewards for hackers, as well as the level of data they can access online and the increasingly ingenious ways they find gaps in security, makes this one of the fastest-growing 'occupations' in the criminal world.

The issue of cyber security has been a regular topic of discussion at TAPA's Worldwide Council meetings and by the end of this year we will have received the recommendations of a working group we tasked with looking into cyber security from a supply chain security perspective. How we plan to move forward and meet the need for new Cyber Security Requirements will be the topic of a future article in our magazine.

We believe that in the best interests of supply chain security, industry standards must be developed and implemented by industry, for industry, and owned, financed and driven by industry. This is based on our experience gained over more than 20 years of offering the leading industry supply chain security standards for facilities and trucking. Consequently, the adoption of TAPA's Standards is now at a record level.

It is important that we continue to serve our members' best interests by developing new Standards that increase their ability to manage risk and prevent crime. In EMEA this month, we launched the highest levels of our new Parking Security Requirements (PSR) to encourage the creation of a growing network of secure parking sites, especially across Europe. Based on over two years of close consultation with the buyers of parking places – Manufacturers and Logistics Service Providers – as well as Parking Place Operators, we are confident PSR satisfies all the levels of secure parking our members have told us they require. Meanwhile, TAPA APAC continues to successfully develop its new Guarding Security Requirements (GSR). Both new Standards will ultimately be considered for adoption by TAPA globally.

This is what being part of the TAPA Family is all about. Whatever the physical distance between our global members, we all share one goal; to minimise losses in our supply chains. It is the sharing of information and best practice, the pooling of our expertise and ideas, and accumulating as much cargo crime intelligence as possible, that makes TAPA the world's leading Security Expert Network for everyone in the supply chain. Operating as one global family will only make us stronger.

Anthony Leimas
Chair, TAPA AMERICAS

Tony Lugg
Chair, TAPA ASIA PACIFIC

Thorsten Neumann
Chair, TAPA EUROPE, MIDDLE EAST & AFRICA

AMERICAS NEWS

EXPERT GROUP TO DELIVER RECOMMENDATIONS ON TAPA CYBER SECURITY STANDARD BY THE END OF 2018

Cyber Security has been one of the hottest topics over the last few years and the level of threat is growing on a daily basis.

TAPA's membership has expressed an interest and need for Cyber Security Requirements and, given the Association's long-standing and highly-respected supply chain Security Standards for Facilities and Trucking, TAPA's Worldwide Council (WWC) believes developing a cyber standard will provide another impactful benefit for its global membership. To date, no one in the industry has addressed cyber security from a supply chain security perspective.

There are market, regional, and government standards that govern IT security implementation and which have components of supply chain risk management (SCRM) included, but nothing addresses the supply chain industry need. Supply Chain Cyber Security is all about leveraging transformational technologies and capabilities (cloud security, blockchain, IoT) to harden IT security systems against determined and capable adversaries, and helping companies comply with new privacy requirements regarding user data, such as the EU's General Data Protection Regulation (GDPR).

The TAPA Worldwide Council, therefore, has decided to look into creating a Cyber Security Standard to enhance the current TAPA Standards. Allen Gear, Vice Chair of TAPA AMERICAS volunteered to create and co-lead a committee in order to review various available standards, including company standards and best practices, and Andrew Parkerson volunteered to chair the Cyber Security committee. This committee is now comprised of 20 TAPA members from all three regions, representing member companies of all sizes, and has been engaged in biweekly conference calls to review existing standards and choosing which standards should be proposed to the Worldwide Change Control Board (WWCCB).

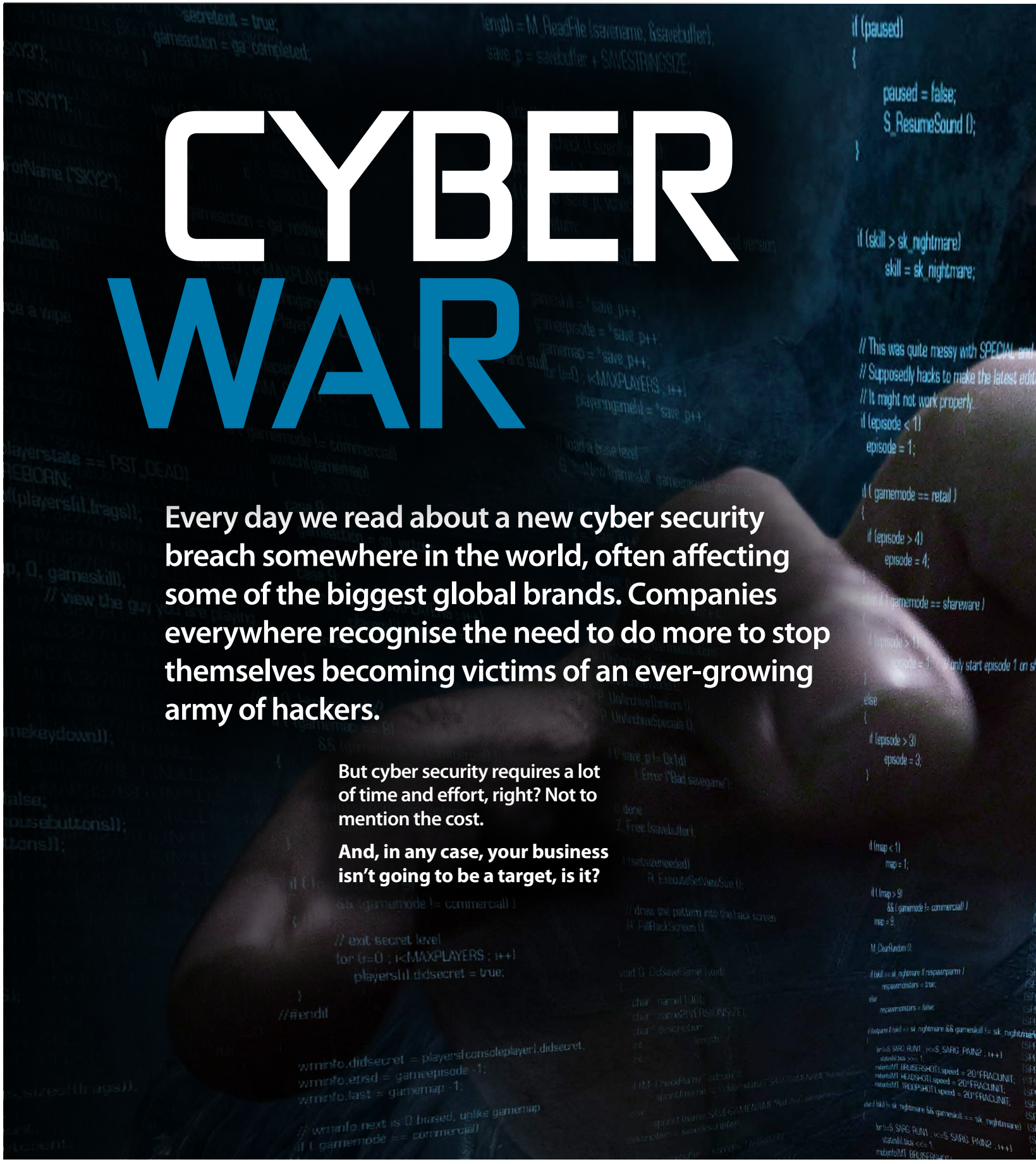

Allen Gear

In considering a new cyber standard, the committee is working on a solution that it capable of crossing all company size boundaries and is applicable, and auditable, in a way which is meaningful to the TAPA membership and the supply chain security industry TAPA serves. It plans to present its recommendations for the WWCCB to review in December.

WELCOME TO THE TAPA FAMILY

Please join us in welcoming the latest members to join TAPA AMERICAS:

Company	Website
Firmenich	www.firmenich.com
Novelis	www.novelis.com
Regeneron	www.regeneron.com
Total Quality Logistics	www.tql.com



CYBER WAR

Every day we read about a new cyber security breach somewhere in the world, often affecting some of the biggest global brands. Companies everywhere recognise the need to do more to stop themselves becoming victims of an ever-growing army of hackers.

But cyber security requires a lot of time and effort, right? Not to mention the cost.

And, in any case, your business isn't going to be a target, is it?

CONTINUED ON PAGE 6 >

For those in need of a hard and fast reality check, a wake-up call, or simply more evidence to put in front of the doubters in their own organisations, Pete Mento (left), Vice President of Global Trade and Managed Services at Crane Worldwide Logistics has shared his own personal insight into the 'Nature of the threat – cargo security & cyber in the new supply chain' at TAPA conferences in the U.S. and Europe, warning that security professionals who do nothing are doing a massive disservice to the future of their businesses.

Frankly, it's a point of view from one of the world's leading experts on International Trade Policy and Supply Chain Security that's impossible to argue against. Earlier this month in Spain, Pete gave his latest presentation to delegates attending TAPA EMEA's Palma conference … and this is what he had to say …

I've spent a lot of time looking at the real threat to security right now and what I've realised is that so much time and effort has been put into physical security and a lot of effort has been put into cyber security but, in reality, the money, time and effort put into cyber security, unfortunately, isn't being put into the right places.

We're very concerned about banking and we're incredibly concerned about the security of personal information but we're not looking at the broader scope of what it would mean if the western world's networking infrastructure was to be attacked. So, it got me thinking about who would do these attacks and where they would hit.

Believe it or not, our infrastructure where supply is affected is probably one of the most likely places that would be hit. I started talking to the sort of people who protect it and I can tell you that one of the things they're most concerned with is the cyber security work that's being done by people in my industry, transportation. They regard one of the weakest areas in the entire cyber security net – regardless of industry – to be supply chains. They couldn't tell us why because it would give up the way they determine security, but their message was chilling.

In the future, it's not going to be about things like bombs, the real target will be the networks that secure the world we live and work in. It's the people that are easily able to hack into them that we're most concerned with because, let's be honest, it's a big, wide, scary world out there and the reality is whoever controls the networks is realistically going to control the world. So, when you're looking at the funding and the amount of time and effort people are putting into network security, think about your own companies, think about the people you're engaged with right now and the amount of time and effort they're putting into it too.

We are now seeing terror organisations coming together and pledging their support to a new generation of central figures, to rally around one leader. Why is this important? It's important because individual terror groups have realised that the physical war they have been engaged in for the past 20 years isn't necessarily getting them any ground. They're looking for secondary threats and more and more ways to be successful. One of the things one of these terror leaders is famous for saying is that he doesn't intend to send his 'soldiers' into physical wars, he plans to arm jihadis with laptops. In his plan to cripple the west, he sees the future as going after our banks and infrastructure because we're weak and we're soft. Imagine, after 9/11, if someone was able to turn off the internet for the day. Imagine the financial impact that would have had.

Being able to hack into a network makes everyone concerned about using that network. It forces every business to consider how they're using it. It slows down commerce worldwide. There is no question that there are terror leaders that intend to use cyber to its fullest to disrupt the business of the west. So, there's a new threat and that threat feels like using cyber.

When I previously spoke at the TAPA conference in the Americas, I asked, 'how many people that are engaged with TAPA have advanced degrees in computer science?' and 'how many people are there in TAPA who are fully engaged in cyber that are not former law enforcement – and that are not people who spend their days worrying about how we're going to secure containers and manage physical security?' Most of us come from that world.

The new Customs-Trade Partnership Against Terrorism (C-TPAT) standards are now just beginning to scratch the surface of cyber – but this threat, and the nature of this threat, is real, and we're only just beginning to realise it. The latest threats that have been happening are

There is no question that there are terror leaders that intend to use cyber to its fullest to disrupt the business of the west. So, there's a new threat and that threat feels like using cyber.

Previously, we've been able to get our arms around all the massive gaps in cargo security because there's something physical to get hold of. With cyber, you can't do that.

only going to put a bigger spotlight on the failure of a lot of the physical cargo security that we have – but what we are beginning to see is a desire to make it better. The issue we face is that there are people who are involved in C-TPAT, in organisations giving advice to customs, that don't want to see the program made any harder because they don't want to make financial investments. They feel enough has been done, even though they understand it could be better.

AEO, on the other hand, continues to be a more robust program as it has always had some semblance of understanding the security of networks because it had a financial component to it.

Previously, we've been able to get our arms around all the massive gaps in cargo security because there's something physical to get hold of. With cyber, you can't do that.

The value of cybercrime is only going to get bigger because of what criminals are beginning to learn. One of the black-hat hackers I spoke with gave me a fascinating insight into how he makes his money by stealing other people's money over the internet, how he steals people's identities and takes their entire bank accounts.

This is a guy who was a Russian national who used to steal prestige $100K cars for a living, take them to a chop shop, take all the risk, be constantly pursued by the police, and then walk away having earned $7-8,000. Now, he told me, he sits in a coffee shop in Odessa and works on his computer and can take a couple of hundred thousand dollars before his day's over with. He doesn't worry about the police and he makes nice pieces of software he can sell to other hackers too. As he said, 'it's a growth business, why wouldn't I want to be involved?'

That growth business is coming from all the places you would imagine, from people in Russia, China, India, Pakistan, Turkey and the United States. And the number of attacks is only going to grow.

The whole idea that we're in a globally networked world supply chain means there should be a greater attitude towards dealing with cyber because this is not a new concept. In America, we've been concerned with cyber security since the 1980s when people started hacking the U.S. Government. The Government started investing in it financially and putting people on it to look for intelligent ways to deal with it because, like everything else, the bad guys are crafty and are going to be able to work around the rules.

Right now, with the trade war that's going on, America's and the west's economy is entirely based on something called innovation – the innovation economy. The physical product doesn't matter anymore. Let's put it like this; what would you rather own right now – shares in a company that makes the ideas other people come up with or stock in the company which comes up with the incredible ideas? You'd probably rather own a share of the company that comes up with the incredible ideas.

As economies, we're moving from focusing on products to focusing more on the ideas because they are what matter most. Our new economy in America is entirely based on protecting these ideas, which is why we're currently in a trade war with China. It's not because of deficits, it's not because we're buying more from China than we're selling. It has to do with protecting IP. And, the Europeans, of course, are just as concerned with that.

There have been wholesale thefts of western ideas through cybercrime, which involve hackers going into servers, stealing millions of dollars of research and either producing those goods themselves or selling the research to someone who wants to make the products in a foreign country. Yes, they have the scientists in these countries and intelligent people but it's just that their innovation economy is not keeping up as quickly.

That's why we're being told to protect our intellectual property with hardened cyber security because more and more things are going to be stolen.

CONTINUED ON PAGE 8 >

There's also the concept of personal security and keeping the intelligent people safe, keeping their information safe. So much of who we are is held on servers now and makes it possible for hackers to blackmail individuals by threatening to use information against them to the point where they are willing to compromise themselves and give up data and information.

We are working in a very resource networked industry and whether you're a customs house broker, a freight forwarder, a transportation provider or a port, since the dawn of network computing we've tried to work with one another because it makes us more efficient. But, you're only as strong as the weakest link in your chain, so if you have tremendous cyber security but you have someone in a port who doesn't, that virus is going to find its way across. And, as you know, many people in the logistics industry have been hit. Recently, another couple of ocean carriers were hit again and it's not going to stop.

There's nothing stopping someone with the will and wherewithal from taking over the navigational abilities of a vessel at sea. Vessels are networked. They are attached to the internet and much of a modern vessel's control systems are networked to the internet. So, it is possible to take over the navigation controls, the engine controls, the life support controls of a vessel. It's only a matter of time before something happens. Ports are also networked, not only to the internet but to each other, and, of course, to government systems as well. Think of the type of debilitating attack that could happen. We're also very concerned about autonomous cars, trucks and planes because as soon as someone can hack into them, they will.

All of the moving pieces and how they inter-connect with one another brings us to what the big fear is. We are constantly seeing terror groups using cybercrime to their advantage, such as to take down parts of security systems in order to cross borders. They're using cybercrime to steal cash and launder money. They also see the use of cyber as a way to create chaos. This is what they want. It's about trying to find some way to crush the will of western people, and that can certainly be done by crushing the supply chain, by breaking down the way we move goods and services.

The numbers are quite ridiculous. In 2016, $228 million of cargo was stolen – in fact this number could be worse. But in 2016, $450 billion was stolen by cybercrime and in 2019, that number is expected to go to $2 trillion.

So, what are we going to do to control that 'back door'? The worst part is there doesn't appear to be any real work done by most companies to deal with cyber threat. And a lot of this is because it requires every individual in your company to become a zealot to cope with these problems, and that takes a lot more time and energy than people are willing to invest.

However, by not doing something, you're doing your business a disservice. Think of what has to happen for someone to steal your cargo physically and resell it versus someone who's able to go in and steal an idea, steal your research, and steal your money online. It's actually a lot easier – and in some cases companies don't even know how much is being stolen. When they find someone has stolen their research, many companies are now hiring hackers to steal it back, which is illegal but they're doing it anyway. In many cases, crimes are not reported because companies don't want to expose the fact that they were exposed. They don't want to let people know they were a soft target and got hit.

Almost all of this stuff is avoidable, but companies don't want to do the simple things to avoid it. So, we're waiting for an absolutely terrible event to take place to prove once and for all that people aren't paying attention.

We are now in a situation where we are seeing more and more people hacking – the newest frontier of hacking is mobile phones because people are not doing a good job of securing them. And, the reason for this is because hacking, in the west, has become a hobby for young people where they think it's fun to break into people's mobile phones, devices and laptops, and if they find something interesting, they sell it.

In many respects, you have to admire the initiative of some hackers. I heard an incredible story of hackers taking a mobile phone, putting it on a drone and then flying it up and down outside hotel rooms at night, while people are asleep, looking for laptops that are still connected to the secured networks of companies, and then trying to hack in through these open connections.

The fact is, however, that so much can be done to prevent this by doing so little. You can protect your company leaps and bounds by doing the bare minimum, but people have to make a conscious effort. If you do the right thing, people are not going to bother to go after you because there are so many other companies that aren't. All you have to do is convince your companies to do the basics – but, in reality, that's going to be hard because they don't feel they're a target.

We spend so much arming the front door because we think people are going to physically steal what makes our companies special. They're going to come in and take our products, our cargo away. But we're leaving the back door completely unsecured, allowing people to come in and steal our ideas, our innovation, the future of our companies.

I applaud all of you for the amazing work that you do keeping your physical plants, people and products secure but if you don't start paying attention to cyber, there won't be those things to take care of in 15-20 years because the future of security is in stealing ideas and concepts in those ones and zeros.

Almost all of this stuff is avoidable, but companies don't want to do the simple things to avoid it. So, we're waiting for an absolutely terrible event to take place to prove once and for all that people aren't paying attention.

EYE-ON-TECH

***Eye-on-Tech* looks at some of the latest security technology updates from leading industry news sources...**

How Artificial Intelligence (AI) is changing video surveillance today

There's a lot of excitement around artificial intelligence (AI) today – and rightly so, reports *Security Informed*. AI is shifting the modern landscape of security and surveillance and dramatically changing the way users interact with their security systems. But with all the talk of AI's potential, you might be wondering: what problems does AI help solve today?

The fact is, today there are too many cameras and too much recorded video for security operators to keep pace with. On top of that, people have short attention spans. AI is a technology that doesn't get bored and can analyze more video data than humans ever possibly could. **Read more…**

What are the challenges of AI for physical security?

Artificial intelligence (AI) is a current buzzword in the physical security market – and the subject of considerable hype. However, AI sometimes gets negative press, too, including dire warnings of its potential and eventual impact from some of our most prominent technology thinkers. *Security Informed* decided to take the issue to its Expert Panel Roundtable: What are the negative impacts and/or new challenges of AI for physical security? **Read their comments here…**

9 in 10 organisations don't have desired security culture

In a new survey on cyber security culture reported in *Infosecurity* magazine, 90% of the nearly 5,000 technology professionals who participated identified a gap in their existing culture and the cybersecurity culture they would like to have. The *Cyber Culture Report* revealed the results of more than 4,800 technology professionals surveyed about security awareness and behaviors in enterprises, particularly how awareness integrates into daily operations and leadership priorities.

According to the survey, a mere 5% of respondents said their organization is well positioned to mitigate both internal and external threats. Only a third (34%) of respondents are aware of the role they play in creating a cyber-aware culture within their organizations, suggesting that many companies are not effectively getting the message out to all employees that they are a first line of defense when it comes to cyber-attacks.
Learn more here…

Making your surveillance cyber secure

In an increasingly-connected world, network and cyber protection have become more important than ever before. It is essential that organizations take the necessary measures to ensure the highest level of security for their networks and IP cameras, encoders, NVRs and DVRs. A new white paper from Hanwha Techwin America explores a number of best practices to strengthen device security and prevent unauthorized access, protecting end users' video surveillance systems and their overall network.

The paper discusses password protection, authentication and encryption, avoiding the cloud, network set-up and configuration, identifying and thwarting attacks, tampering detection and updating firmware.
Access the white paper here

Most IT pros fear AI-powered attacks

Over 80% of security professionals are concerned about the prospect of attackers using artificial intelligence (AI) against their organization, according to new research from the global information services provider, Neustar. It polled 301 IT and security professionals across EMEA and the U.S. to compile its latest International *Cyber Benchmark Index*. It found that although 87% of respondents agreed AI would help them improve cyber-defenses, a similar number (82%) claimed to be nervous about the prospect of it being used by black hats against them in the future.

Respondents feared the prospect of stolen data (50%) resulting from attacks most of all, although loss of customer trust (19 %), unstable business performance (16 %) and extra costs (16%) all figured highly. **Read more…**

83% avoid a business following breach and 21% never return

Almost half (44%) of U.S. consumers have suffered the negative consequences of a security breach or hack, according to new research conducted on behalf of secure payments provider to contact centers, PCI Pal. The findings suggest that the combination of high-profile recent breaches, headlines devoted to new data privacy regulations such as the GDPR and California Privacy Law, and personal experience, have put security concerns front and center for American shoppers.

The research found that 83% of consumers will stop spending with a business for several months in the immediate aftermath of a security breach or a hack. Even more significantly, over a fifth (21%) of consumers will never return to a brand. **Read more…**

How to work with hackers to make your company more secure

Check out this fascinating story from *Security* magazine. The author says: "For most ethical hackers, including myself, hacking doesn't feel like work. We're a community of puzzle-solvers – curious and eager to share the vulnerabilities we uncover that can have repercussions for your company and your customers."
Click here to read more…

Want to contribute to Eye-on-Tech? Let us know at info@tapaemea.org. Our objective is to bring you information that really matters to Supply Chain Security Experts.
Please note that none of the items covered in this section are endorsed by TAPA.

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 …

Lina Li, TAPA APAC

My name is Lina Li and I am currently working for Signify (formerly Philips Lighting) as Head of Security for Asia.

Out of my 17 years' working experience in the security industry, I've spent 14 years on either supply chain security-focused activities or having securing the supply chain as part of my role.

Starting from my first job to manage Shanghai Integrated Warehouse and Freight Security for China at Intel, I connected my career life with TAPA. Since our company was one of the pilot companies to launch the first version of TAPA Facility Security Requirements (FSR), I was honored to become one of the first batch of FSR trainees and to then be able to introduce and promote this industry standard to more and more of our logistics service providers.

After I moved my career from the buyer industry to the logistics service provider industry, I became a TAPA APAC Board Member in 2013. I have witnessed how the TAPA Standards have been gradually accepted and recognized by more and more buyers, suppliers and service providers. Especially after several rounds of revision, they were more fit for groundwork operations and able to better address those common loopholes in warehouse security management, including introducing more industry best practices. Through integration of the TAPA FSR & TSR Requirements into our own company supply chain security program, we were able to streamline the management of supply chain security performance towards different service providers and also adopt industry intelligence and benchmarking to earlier spot different security risk exposures in our supply chain.

Personally, I have also benefited from actively participating in different TAPA working groups during the past five years. This has not only helped me keep abreast of the latest supply chain security trends and technologies, but also expanded my network through which I can discuss a lot of common issues with counterparts in the industry and share different practices.

Starting this year, it's my pleasure to lead the APAC training committee under the support of Mr. Herdial Singh, and I have become a member of TAPA's Worldwide Change Control Board (WWCCB).As you may know, a new GSR (Guarding Security Requirements) has been launched as an APAC initiative and piloted in a couple of countries thanks to the great efforts of a group of security professionals. Meanwhile, several new global initiatives are also at the planning stage, i.e. modular standards, multi-site certification and cybercrime standards etc. We believe that through the consistent delivery of up-to-date, high-quality standards and by bringing the utmost value to our members, TAPA can unite more and more industry players to minimize cargo losses from supply chains.

In the last 10 years, I have seen more and more women joining the security industry, especially from China. These successful ladies have brought diversity, energy and ingenuity into this male-dominated industry. Here, I'd like to advocate more female security practitioners to join TAPA and our various APAC working committees. We will provide you with a great international stage to present your talent and demonstrate your leadership. I'm looking forward to hearing from you.

'We believe that through the consistent delivery of up-to-date, high-quality standards and by bringing the utmost value to our members, TAPA can unite more and more industry players to minimize cargo losses from supply chains.'

APAC NEWS

SANKYU SINGAPORE BECOMES THE FIRST COMPANY TO ACHIEVE TAPA APAC'S GUARDING SECURITY REQUIREMENTS

SANKYU SINGAPORE is the first member company to achieve the TAPA APAC's 2018 GSR (Guarding Security Requirements) Standard.

Since the GSR Standard was formally launched earlier this year, a number of companies have signalled their intention to participate in the pilot self-certification program. Currently, two further Manufacturer (Buyer) members, two Logistics Service Providers and several Security Service Providers are also engaged in the GSR pilot study.

The GSR was developed to close the gaps identified between the TAPA FSR and TSR Security Requirements and the Security Service Provider (SSP). The evolution of this standard was driven by buyer members in the APAC region.

Research showed that guarding companies manning TAPA certified sites were generally unaware of TAPA's Security Standards and had difficulty in understanding the requirements. This was especially apparent where the SSP was responsible for meeting TAPA's requirements relating to responsibilities such as Access Control Management, Perimeter Security, Guard House Duties, CCTV and Alarm Monitoring. "It was apparent that the TAPA Standards did not cross into Guarding SOP's and visa-versa. The TAPA Guarding Security Standard was developed with the view to bridge the gap and to provide a benchmark for guarding requirements in whichever country or city a site is located in," said TAPA APAC Chairman, Tony Lugg.

The pilot TAPA Guarding Security Standards (GSR 2018) operating in Asia Pacific offer a solution for Buyer members to integrate their security and safety protocols between Security Service Provider (SSP) and guarding security companies' service standards, including:

- A contractual written service level agreement and adherence of best practices 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
- Reporting of Key Performance Indicators (KPI) to drive efficiencies
- Ensuring SSPs only deploy guards who are sufficiently trained and qualified to carry out their duties and roles, especially in relation to TAPA certified sites
- To facilitate a process of continual improvement for the benefit of TAPA members
- Creating a cost-effective guarding service with a clear scope of services
- Improving the efficiency of staff, reducing risk and improving response

Tony Lugg added: "The goal of the GSR Working Group has been to seamlessly integrate the GSR with other TAPA Standards. Guarding Services companies are a major part of security in the supply chain and this pilot will allow us to test all areas and make improvements where required. In this regard, we are pleased to be working with the Singapore Institute of Material Management (SIMM) and using their expertise in this area."

Any Buyers, Logistics Service Providers or SSPs interested in piloting the GSR Standard should contact **roger.lee@tapa-apac.org** or **tony.lugg@tapa-apac.org**

TAPA APAC members can attend the relevant training as part of their training entitlement.

Alvin Matabang, Amkor Technology Security Manager, Nilo Pomaloy, Director Shieldcoach Security & TAPA Philippines Service Centre, Tony Lugg, Chairman of TAPA APAC, Dr. Dan Lachica, SEIPI President, Mabelle de la Cruz, SEIPI Lead for Training and Human Resources, and Katrina Magcalayo, Industry Specialist, SEIPI.

TAPA ADDRESSES SEIPI MEMBERS IN THE PHILIPPINES ON EMERGING SUPPLY CHAIN THREATS

Members of the Semiconductor and Electronics Industries of the Philippines, Inc., (SEIPI) have been updated on emerging risks to their supply chains as well as the benefit of TAPA's Security Standards to minimize cargo losses.

SEIPI, which has over 320 manufacturing company members including leading global brands, organised the presentation by Tony Lugg, TAPA APAC's Chairman, in conjunction with the TAPA Service Centre in the Philippines, managed by Nilo Pomaloy and Pol Camacho of Shield Coach Security Company. In 2018 to date, the Service Centre has provided FSR and TSR training to over 50 TAPA members.

EUROPE, MIDDLE EAST & AFRICA REGION

CARGO CRIME MONITOR

CARGO THEFT BY COUNTRY

September 2018

Belgium	3 (1.3%)
Czech Republic	1 (0.5%)
France	1 (0.5%)
Germany	7 (3.1%)
Italy	1 (0.5%)
Netherlands	28 (12.6%)
Spain	1 (0.5%)
Sweden	1 (0.5%)
United Kingdom	178 (80.5%)

Number of incidents in month

MOTORWAY SERVICE AREAS

x60

60 of the 178 cargo crimes reported in the United Kingdom in September occurred at Motorway Service Areas (MSAs)

€139,505

Average loss for the 9 major cargo crimes reported to TAPA's Incident Information Service (IIS) in EMEA in September 2018

€5,900,218

Total loss for the 172 or 77.8% of crimes stating a value

+33.9%

Year-on-year change in the number of recorded cargo crimes vs. September 2017

221

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

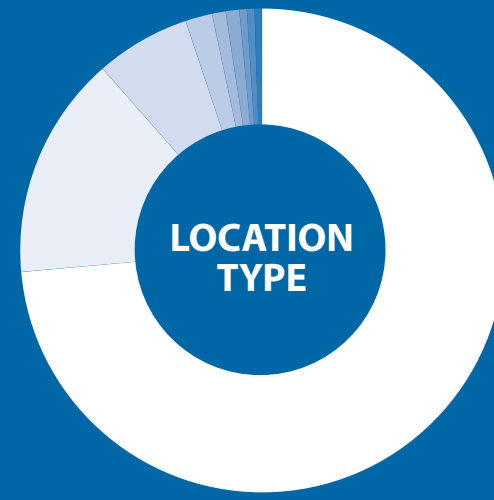
€281,233

Biggest single loss - Theft of Trailer loaded with Clothing & Footwear from an Authorised 3rd Party Facility in West Bromwich in the UK West Midlands on 20 September.

Number of countries in EMEA reporting incidents

9

Theft from Vehicle	196 (88.6%)
Theft from Trailer	10 (4.5%)
Theft of Vehicle	5 (2.3%)
Theft of Trailer	3 (1.3%)
Truck Theft	2 (0.9%)
Theft from Facility	2 (0.9%)
Theft of Container	1 (0.5%)
Theft from Train	1 (0.5%)
Theft from Container	1 (0.5%)



Unsecured Parking	163 (73.7%)
Unknown	33 (14.9%)
En Route	14 (6.3%)
Destination Facility	4 (1.8%)
Secured Parking	2 (0.9%)
Authorised 3rd Party Facility	2 (0.9%)
Services 3rd Party Facility	1 (0.5%)
Railway Operation Facility	1 (0.5%)
Aviation Transportation Facility	1 (0.5%)

21

Crimes in EMEA recording a loss value of between €50,000 & €100,000 produced a combined loss total of **€1,359,135**

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

€34,303 AVERAGE LOSS VALUE LAST MONTH

73.7%

Or 163 of the recorded incidents took place in Unsecured Parking locations

MODUS OPERANDI USED IN LATEST CARGO THEFTS:

Intrusion	204 (92.3%)
Theft from Moving Vehicle	8 (3.6%)
Unknown	5 (2.3%)
Violent & Threat with Violence	4 (1.8%)

CONTINUED ON PAGE 14 >

CARGO THEFTS RISE 33.9% YEAR-ON-YEAR IN SEPTEMBER AND LOSSES WITH A VALUE HIT €5.9M AS SUPPLY CHAINS ARE TARGETED IN NINE COUNTRIES IN EMEA

The number of cargo theft incidents reported to TAPA's Incident Information Service (IIS) in the Europe, Middle East and Africa (EMEA) region in September rose 33.9% year-on-year to 221.

The 172 or 77.8% of these crimes recording a value produced a total loss of **€5,900,218,** with an average per incident of **€34,303.**

Nine of these thefts were recorded as major incidents with individual loss values of **€100,000** or more, totalling **€1,255,551** or an average of **€139,505.** During the 30 days of September, a further 21 reported crimes stated a loss value of between **€50,000** and **€100,000** and accounted for **€1,359,135** of the monthly total, an average of **€64,720.**

The biggest recorded loss in EMEA last month was a Theft of Trailer incident from an Authorised 3rd Party Facility in West Bromwich in the West Midlands region of the United Kingdom. According to IIS intelligence, the offenders broke into a secured yard on 20 September and forcibly removed the trailer from a tractor unit, damaging the truck in the process. They escaped with Clothing & Footwear worth **€281,233.**

This was one of seven major cargo crimes recorded in the UK during the month. The other thefts included:

€151,892

On 1 September, another load of Clothing & Footwear was stolen from a truck parked in a layby on the A2 in Canterbury, Kent, after thieves sliced open the tarpaulin side of the vehicle.

€129,547

A shipment of cornflakes and kitchen towels disappeared after thieves using two tractor units with cloned licence plates took trailers from an unsecured parking location in Lockerbie, Scotland on 15 September.

€126,330

Barton Park motorway services in North Yorkshire was the scene of this cargo theft on 3 September. Offenders targeted a parked and attended truck, cutting open the curtain side of the vehicle to steal its load of televisions. The location is close to junction 56 of the A1(M).

€114,576

Computers/Laptops were stolen from another vehicle stopped in an unsecured parking location on 20 September. The curtain side of the truck was cut open to reach the cargo after the driver had parked in a layby on the A14 in Kelmarsh, Northamptonshire.

€111,463

The same M.O. resulted in the loss of a shipment of gin and tequila on 3 September from a truck in an unsecured parking location in Derby, East Midlands.

€100,510

The second major cargo crime at a UK motorway service area during the month was recorded on 18 September and resulted in the loss of Tyres from a vehicle parked at Leicester Forest East MSA on the M1 motorway in the East Midlands.

The two other major losses in September were recorded in Sweden and Germany. TAPA has been asked not to publish information on the first of these crimes. The other incident – another 'curtain-cutting' crime – saw thieves escape with televisions valued at **€100,000** from a truck in an unsecured parking location in Duisburg in the German state of North Rhine-Westphalia.

The overwhelming majority of cargo crimes in EMEA continue to involve Theft from Vehicle incidents. These accounted for 196 or 88.6% of thefts reported to the IIS database last month.

Losses of between €50,000 and €100,000 during the month also included these Theft from Vehicle crimes, which were all recorded in the UK and mostly involved 'curtain-cutting':

- **€98,053** – Shoes and trainers stolen in Maidstone, Kent, on 10 September
- **€92,348** – Unspecified cargo in Castleford, West Yorkshire on 26 September
- **€73,426** – Fitness equipment stolen in Normanton, West Yorkshire, on 26 September
- **€73,125** – Clothing & Footwear from a Destination Facility in Pontefract, West Yorkshire, on 13 September
- **€72,296** – A shipment of gin stolen from a truck at Woolley Edge motorway services in Wakefield, West Yorkshire, on 25 September
- **€66,162** – Tyres stolen from a truck at Leicester Forest East MSA on 22 September
- **€65,824** – Batteries taken from a vehicle at Cambridge MSA on 7 September
- **€63,406** – Wine stolen from a truck parked in a layby on the A50 in Ashton-on-Trent, Derby, on 7 September
- **€63,259** – Another shipment of wine stolen from a vehicle in Northampton, East Midlands, on 29 September
- **€63,218** – Another theft of Tyres from a truck in a layby in Whitwell, Derbyshire, on 5 September

Overall, losses were reported in 14 TAPA IIS product categories, including four with double-digit crime rates:

- Food & Drink – 35 incidents, 15.9% of the September total
- Tobacco – 20 incidents, 9.1%
- Clothing & Footwear – 16 incidents, 7.3%
- Furniture/Household Appliances – 10 incidents, 4.5%

The overwhelming majority of cargo crimes in EMEA continue to involve Theft from Vehicle incidents. These accounted for 196 or 88.6% of thefts reported to the IIS database last month. Most of these losses – 163 or 73.7% - occurred when trucks stopped in unsecured parking locations. Intrusion, in the form of tarpaulin cutting or thieves forcing open the rear doors of vehicles, was the most recorded M.O. Eight other crimes gave an M.O. of Theft from Moving Vehicle, which all involved thieves targeting shipments of cigarettes while they were en route in the UK.

In total, freight losses were reported to TAPA's IIS in nine countries in EMEA. Of the overall total, 206 or 93.1% of these incidents occurred in just two countries, the UK (178) and the Netherlands (28).

In the UK, 60 of the 178 freight thefts took place at motorway service areas. Overall, the value of cargo losses across the country - **€5,634,718** - accounted for almost the entire EMEA loss value in September. The most stolen products in the UK included Food & Drink (34 incidents), Tobacco (18) and Clothing & Footwear (15).

CONTINUED ON PAGE 16 >

Whilst the East Midlands region was the location with the most recorded cargo crimes in the UK last month - 87 or 48.8% of the total – there was a significant rise in the number of incidents reported in Yorkshire & The Humber. Most notably, the TAPA IIS database was notified of 14 incidents at Woolley Edge motorway services in Wakefield over a 10-day period with a combined loss of **€392,726** as thieves stole shipments of soft drinks, clothing, gin, tyres, towels and brandy. Pontefract was another crime 'hotspot' in Yorkshire, recording 11 incidents in two weeks involving vehicles parked at truck stops, in laybys and on industrial estates. These crimes – which involved losses of pharmaceuticals, boiler parts, vegetables, cosmetics, training shoes and soft drinks – produced a total loss of **€185,207.**

Limburg was the province of the Netherlands to record the highest number of incidents, 10 in total. There were also multiple cargo crimes reported in South Holland, eight in total, and North Brabant, the scene of a further six thefts. Products targeted in the Netherlands included metal, televisions, jeans, cigarettes, glasses, tyres, batteries, computers, sports equipment, dishwashers, beer, toothbrushes and Christmas decorations.

Most where stolen in Theft from Vehicle crimes.

Crime hotspots in the Netherlands in September included the following highways:

- A2 – Maarheeze in North Brabant as well as Echt and Eijsden in Limburg
- A16 – Zevenbergen in North Brabant
- A67 – Bladel in North Brabant and Venlo in Limburg
- A73 – Roermond in Limburg

Other crimes in the EMEA region included:

- All seven freight thefts in Germany saw thieves targeting vehicles, mostly cutting the tarpaulin curtains of trucks to steal products including copper, household appliances and DVDs. Losses were recorded in North Rhine-Westphalia, Thuringia, Bavaria, Brandenburg and Lower Saxony
- Three Theft from Trailer crimes in Belgium targeting cigarettes and car parts. Two of these incidents were recorded in Hainaut province and the other in Namur
- In France, offenders broke into a compound and threatened warehouse staff with iron bars before escaping with unspecified cargo from an Authorised 3rd Party Facility in Jonage, Lyon

PRODUCT CATEGORY	No	%
Unspecified	88	39.9%
Food & Drink	35	15.9%
Tobacco	20	9.1%
Miscellaneous	16	7.3%
Clothing & Footwear	16	7.3%
Furniture/Household Appliances	10	4.5%
Cosmetics & Hygiene	7	3.1%
No Load	7	3.1%
Tyres	6	2.7%
Sports Equipment	3	1.3%
Metal	3	1.3%
Computers/Laptops	3	1.3%
Tools/Building Materials	2	0.9%
Pharmaceuticals	2	0.9%
Car Parts	2	0.9%
Phones	1	0.5%

- The only recorded incident in Italy saw thieves take a vehicle loaded with steel on 3 September from a Services 3rd Party Facility in Terni, Umbria
- El Molar, Madrid, was the location of the single cargo crime reported in Spain, involving the theft of electrical tools from a vehicle in a truck park on 11 September

- Another 'curtain-cutting' incident in the Czech Republic enabled thieves to steal a shipment of DVDs from a truck in Poděbrady.

ASIA PACIFIC INCIDENT NEWS

Three cargo thefts in India result in losses of more than $198,000

TAPA's Incident Information Service (IIS) recorded three cargo thefts in India last month, including one major loss involving a Theft from Facility of cosmetics valued at US$137,050 on 15 September.

Five men were subsequently arrested in Mumbai for stealing two containers loaded with cosmetics, which they sold in a local market. Fake customs clearing documents were used to transport the two containers from the Nhava Sheva customs house.

Three days earlier, another Theft from Facility resulted in the loss of 45 barrels of diesel and base oil used for ships along the Dadar Sagari, Mandawa, Revas and Dharamtar coastline. A gang of 10 people have been arrested for the crime, accused of collaborating with cargo ship crew members. The value of the goods stolen was recorded as $61,000.

TAPA's IIS was also notified of the theft of phones from an Aviation Transportation Facility in Delhi on 19 September.

In all three cases, the M.O. was recorded as Internal.

EVERY INCIDENT REPORT COUNTS

REMEMBER: TAPA's IIS incident intelligence database does not require you to publish your name or the name of any company or companies that are victims of crime. You will simply be asked to confirm as much detail as possible relating to:

- Date of incident
- Incident category, i.e. Theft from Vehicle
- Modus operandi used by offenders
- Incident description
- Product category
- Product details
- Loss value
- Type of Location where the incident occurred, i.e. Unsecured Parking
- The town, district, region and/or postcode of where the crime occurred
- Country
- A link to a media report on the crime (if there is one)

Using TAPA's IIS reporting tool is quick and easy. Learn more by watching our IIS Explainer Video

IIS

WATCH NOW

STANDARDS FAQs #14

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.

When you send a question to TAPA about our Security Standards, we keep a record of all of our responses to the originator. As we have just launched the Parking Security Requirements 2018 (PSR) in EMEA, this month's article answers some of your initial questions on the new Standard.

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**

Question 1.

What is the PSR Security Standard and who is it intended for?

Answer: The Parking Security Requirements (PSR) is the latest TAPA Security Standard. It is for the operators of truck parking areas that want to use an industry standard which is widely recognised by shippers and the logistics industry. Our aim is to significantly grow the footprint of available TAPA-approved secure parking areas to help protect drivers, vehicles and loads when they are required to take rest breaks.

Question 2.

I saw an older version of PSR. What's new in PSR 2018?

Answer: The older version was PSR 2017 and was a pilot version. It contained one security level and numerous options on how to become involved in the scheme. PSR 2018 now contains three security levels and the involvement of approved Independent Audit Bodies (IABs) to complete the certification process. As with FSR and TSR, there is also a self-certification option for PSR Level 3.

STANDARDS SUPPORT

Question 3.

Why do we need PSR?

Answer: In the EMEA region alone in 2017, 70% of all cargo crimes reported to TAPA's Incident Information Service (IIS) involved trucks which had stopped in unsecured parking locations. The number of these incidents – 2,019 in total – also represented a 90% increase in these incidents over the previous year. With more and more trucks on the road, the lack of suitable parking areas is making cargo vehicles an attractive and, often, relatively easy target for criminals.

Many previous initiatives to tackle the insufficient level of secure parking have failed. In response to TAPA members' concerns – and based on the Association's success with its other Facility Security Requirements (FSR) and Trucking Security Requirements (TSR), TAPA decided to develop and manage its own secure parking standard to benefit its members as well as the wider supply chain industry.

PSR has been developed in close consultation with TAPA's Manufacturer and Logistics Service Provider members – buyers of parking places – as well as with Parking Place Operators and we now have a recognised Standard for secure parking that has been created by the industry, for the industry.

We hope our efforts will convince hundreds of parking place operators to join our scheme and provide a choice of effective and affordable parking which meets all of the security level requirements of our industry.

Question 4.

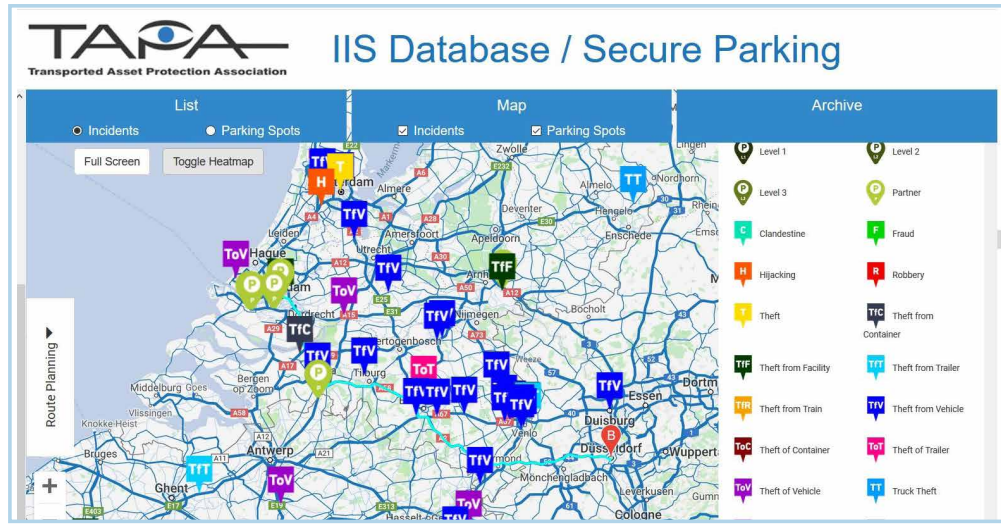
Is PSR a global standard?

Answer: We have just officially launched PSR in the EMEA region. We are working with our TAPA colleagues in the AMERICAS and ASIA PACIFIC to help them consider also adopting PSR. We know of several countries in Asia which are already very interested in the PSR Security Standard and hope to see its adoption outside of EMEA soon. We will continue to send out regular updates on the growth and use of PSR.

Question 5.

How is PSR linked to incident data?

Answer: The PSR Standard comes complete with some valuable additional tools to help TAPA members plan secure transportation routes. Members of TAPA with access to our IIS are now able to access our new Security Parking Online Tool (SPOT), a risk management mapping solution which allows a user to enter a route, identify incidents on or close to the intended route, and then find the nearest TAPA PSR-approved secure parking sites. The tool will be populated with every parking place which meets the requirements of the TAPA Standard.



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 FSR or TSR 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	DHL Express (Austria) GmbH	AT	Guntramsdorf	A
FSR	DHL Express (Poland)	PL	Warsaw	A
FSR	DHL Express Italy Srl	IT	Malpensa (VA)	A
FSR	DHL Freight	DE	Nürnberg	C
FSR	DHL Freight (Sweden) AB	SE	Varnamo	C
FSR	DHL Freight (Sweden) AB	SE	Gavle	C
FSR	DHL Freight (Sweden) AB	SE	Sundsvall	C
FSR	DHL Freight GmbH	DE	Köln	C
FSR	DHL Freight GmbH	DE	Menden	C
FSR	DHL Freight International & Voigt GmbH	DE	Neumünster	C
FSR	DHL Freight Spain S.L.	ES	Madrid	A
FSR	DHL Hub Leipzig GmbH	DE	Schkeuditz	A
FSR	DHL International Express	FR	Chemillé	A
FSR	DHL Parcel Pontevedra Spain S.L.U.	ES	Vigo (Pontevedra)	A
FSR	DHL Parcel Sevilla Spain S.L.U.	ES	Carmona (Sevilla)	A
FSR	DHL Supply Chain Benelux	NL	Beringe	A
FSR	DPDgroup UK Ltd	GB	Carlisle	A
FSR	DPDgroup UK Ltd	GB	Quedgeley	A
FSR	DPDgroup UK Ltd	GB	Kimnel Bay	A
FSR	DPDgroup UK Ltd	GB	Glasgow	A
FSR	GVT Transport & Logistics Alkmaar B.V.	NL	Alkmaar	B
FSR	Panalpina SA	LU	Munsbach	C

TSR	Company Name	Country	Category
TSR	H.Essers Security Logistics B.V.	NL	Level 1,2 & 3 / Category Large
TSR	Franz Wirtz GmbH	DE	Level 1 & 2 / Category Medium

WELCOME TO THE TAPA FAMILY

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

Company	Country	Website
CanTrack Global Ltd	GB	www.CanTrack.com
Transportes Frigorificos RP	ES	www.tfrp.eu
Truck Parkings Rotterdam Exploitatie BV	NL	www.truckparking-rotterdam.com

LATEST FSR & TSR SECURITY CERTIFICATIONS

ASIA PACIFIC REGION

FSR	Company Name	Country	City	Class
FSR	Agility Logistics Limited	Hong Kong	Hong Kong	A
FSR	Converge Asia Pte Ltd	Singapore	Singapore	A
FSR	DHL Aviation (Hong Kong) Limited	Hong Kong	Hong Kong	A
FSR	DHL Aviation Services (Shanghai) Co.,Ltd.	China	Shanghai	A
FSR	DHL Express	Australia	Auckland	A
FSR	DHL Express	New Zealand	Christchurch	A
FSR	DHL Express	New Zealand	Wellington	A
FSR	DHL Express (India) Pvt Ltd	India	Goa	A
FSR	DHL-Sinotrans International Air Courier Ltd. Hubei Branch	China	Wuhan	A
FSR	DHL-Sinotrans International Air Courier Ltd. HQW Service Centre	China	Shanghai	A
FSR	DHL - Sinotrans International Air Courier Ltd. PEK (West Area) Express	China	Beijing	A
FSR	DHL-Sinotrans International Air Courier Ltd. PEK Second Branch	China	Beijing	A
FSR	Mentor Media Ltd.	Singapore	Singapore	A
FSR	Nippon Express NEC Logistics Taiwan Ltd.	Taiwan	Taoyuan	A
FSR	Pantos Logistics Singapore Pte Ltd	Singapore	Singapore	A
FSR	Schenker Australia Pty Ltd	Australia	NSW	A
FSR	Schenker Logistics (Xiamen) Co., Ltd.	China	Fujian	A
FSR	Shenzhen Fertile Plan International Logistics Company Limited (Jusda)	China	Shenzhen	A
FSR	Shenzhen Fertile Plan International Logistics Company Limited NanNing Branch (Jusda)	China	Nanning	C
FSR	SJ Logistics Limited	Hong Kong	Hong Kong	B
FSR	Sunstar Supply Chain (Shenzhen) Co., Ltd.	China	Shenzhen	C
FSR	YCH Distripark Sdn Bhd	Malaysia	Pulau Pinang	A
TSR	Company Name	Country	City	Class
TSR	Bondex Logistics Co., Ltd.	China	Zhengzhou	Level 2
TSR	KPS World Transportation Limited	China	Shenzhen	Level 2
TSR	Shenzhen Eastern Worlwide Logistics Co., Ltd.	China	Shenzhen	Level 2
TSR	Shenzhen Shengchanglong Container Cargo Transportation Co.,Ltd	China	Shenzhen	Level 2

WELCOME TO THE TAPA FAMILY

Please join us in welcoming the latest members to join TAPA APAC:

Company	Country	Website
Aramex International L.L.C.	Singapore	www.aramex.com
Bondex Logistics Co.,Ltd	China	www.bondex.com.cn
Cardinal Health Products India Pvt. Ltd.	India	www.cardinalhealth.com
Golden Triangle Security Services Sdn Bhd	Malaysia	www.goldentrianglesecurity.com
Hong Kong Air Logistics Co., Ltd	Hong Kong	www.seaairlogistics.com
iG Logistics Pte Ltd	Singapore	iglogistics.com.sg
Maxitulin Sendirian Berhad	Malaysia	maxitulin.com
Pantos Logistics Malaysia Sdn Bhd	Malaysia	www.pantos.com
Shanghai TAKE Logistics Co., Ltd.	China	
Shenzhen FuShiLin Logistics Co.,LTD.	China	
U Performa Resources PLT	Malaysia	www.u-performa.com
Uber Singapore	Singapore	www.uber.com

AMERICAS NEWS

HEALTHCARE READY KICKS OFF TAPA AMERICAS EDUCATIONAL WEBINAR PROGRAM

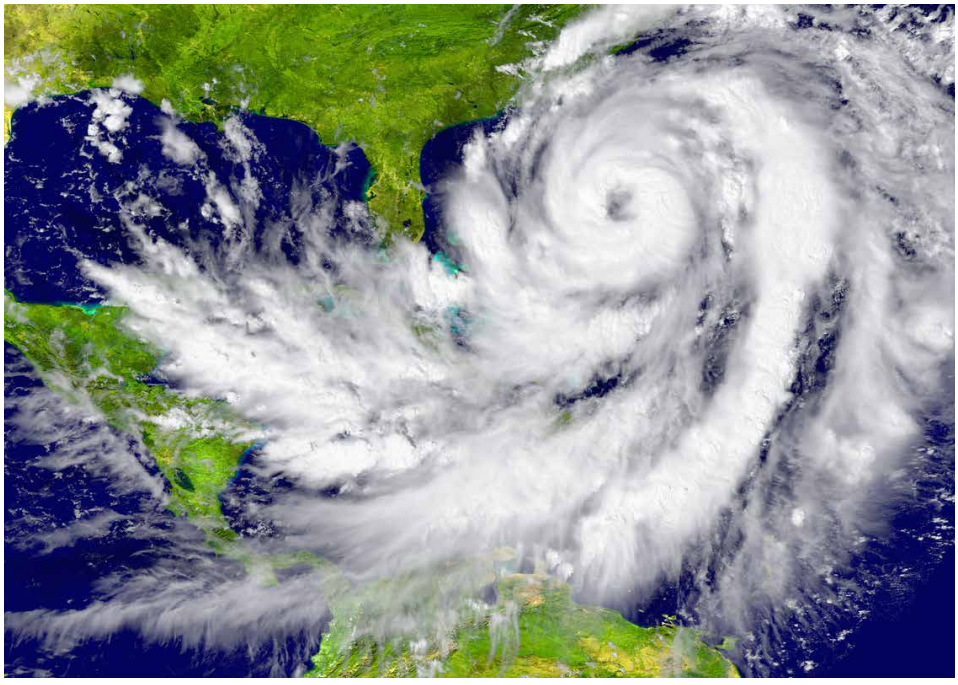
TAPA AMERICAS' Education Committee, chaired by George Latos, has developed a series of webinars to expand the knowledge leadership and development of supply chain security professionals. These webinar sessions are designed to discuss trends in different sectors, educate members on best practices, and open dialogue between all stakeholders in the effort to reduce cargo theft and secure supply chains. The webinars target both the general interests of all stakeholders as well as specific, vertical markets and industries.


Nicolette A. Louissaint

The first webinar in August, presented by Nicolette A. Louissaint, Ph.D., Executive Director of Healthcare Ready, produced an excellent response after it summarized recovery measures following the 2017 hurricane season as well as lessons learned and preparations for 2018 and beyond.

TAPA members work with Healthcare Ready to respond to natural disasters and ensure the distribution of life-saving medicines and drugs on a timely basis. Dr. Louissaint shared with attendees how Healthcare Ready prioritizes locations, tracks the status of existing distribution networks, and provides information to decision makers as to the current and future situation of a disaster and the need to build ad hoc supply chains to deliver medicines and drugs while pharmaceutical companies reestablish their supply chains. TAPA members subsequently had a chance to put the lessons learned from Dr. Louissaint into practice during Hurricane Florence, which hit the southeastern U.S. in September.

The Education Committee is now working on future webinars to address cargo crime investigations and other current supply chain security issues of interest to TAPA members. Each webinar will be recorded and archived for members to view on-demand should they be unable to attend the live presentation.



UPCOMING TAPA MEETINGS AND PRESENTATIONS

TAPA Americas 2018 T2 Meeting/Law Enforcement Conference is taking place on October 30-31 and will be reported in the next issue of *Vigilant*. The meeting at the Delray Beach Marriott Hotel in Florida is the annual law enforcement focused event which brings TAPA members together with the public and private sector. Presentations will include cargo theft task force updates, best practices, and new reports on trends in cargo theft and technology.

Earlier this month, TAPA AMERICAS' Dave Wilt provided a TAPA update to delegates at the National Insurance Crime Bureau (NICB) Cargo Crime Summit in Memphis, Tennessee, which was attended by leading cargo crime authorities from across the United States, discussing patterns and practices of cargo thieves, recent case studies and practices to combat cargo theft.

POLICE ARREST 14 IN MIAMI

Prosecutors in Miami have charged 14 people with being part of an 'incredibly organized' cargo crime ring which has reportedly been responsible for losses involving furniture, soft drinks, shoes, tires and food products over the past two years.

The case was made by Miami-Dade police's cargo-theft task force, along with detectives from Jacksonville, Lee and Charlotte counties and the Georgia Bureau of Investigation, according to a media report. The police investigation, prosecutors stated, has uncovered a prolific ring of Miami cargo thieves who targeted trailers throughout Florida and Georgia. More than $5 million in property was allegedly stolen, of which police have recovered $2.2 million worth, the media source states.

EMEA NEWS

TAPA EMEA LAUNCHES LEVELS 1 & 2 OF NEW SECURE PARKING PROGRAMME TO REDUCE CARGO CRIME IN EUROPE

Levels 1 & 2 of TAPA's new Parking Security Requirements (PSR) went 'live' in EMEA on 15 October, giving Parking Place Operators (PPOs) four ways to participate in the Association's secure parking programme:

- **PSR Level 1** – high security protection with a formal certification
- **PSR Level 2** – mid-level security protection with a formal certification
- **PSR Level 3** – lowest security protection with a formal certification
- **PSR Partnership Declaration** – minimum entry level not requiring a formal certification

The new TAPA Security Standard aims to address the significant growth of cargo crimes involving trucks which have stopped in unsecured parking locations, particularly in Europe, which continues to suffer from a severe lack of secure parking sites. In 2017, cargo thefts reported to TAPA's Incident Information Service (IIS) produced losses in excess of **€100 million** and 2,019 or 70.1% of these crimes occurred as a result of unsecured parking.

TAPA EMEA members can identify PSR certified sites and PSR partners using the new Secure Parking Online Tool (SPOT) which allows them to set a specific transport route and then see the cargo crime incidents recorded along the route as well as the nearest TAPA PSR parking locations.

For further information about TAPA's PSR please contact info@tapaemea.org

MEETING & EVENTS

- TAPA EMEA Chairman, Thorsten Neumann participated in a webinar on Supply Chain Security hosted by the International Union of Marine Insurance (IUMI) to talk about cargo crime trends and TAPA's latest initiatives to help companies reduce losses. Over 50 IUMI members registered for the webinar
- 
Laurence Brown (left), Executive Director of TAPA EMEA, will address the 3rd Annual Supply Chain Risk Management conference in London in November, presenting the importance of proactive partnerships in mitigating risk
- TAPA will be hosting a meeting of the Russia Working Group in St. Petersburg in December. More information will be provided to members shortly.

NEXT TRAINING

TAPA EMEA's next training course will cover its Trucking Security Requirements (TSR) and will be conducted in Italian in Milan on 20 & 21 November. For more information, go to the Industry Standards section of the Association's website at **www.tapaemea.org**

CAN YOU HELP?

TAPA EMEA's Standards Team is looking to recruit a pool of Subject Matter Content Experts (SMCE) to resource projects with the best qualified people and provide technical advice. It is also seeking people who are interested in joining the Standards Team 'wait list' who can step in when positions become available and ensure continuity of support for members' TAPA certification programmes.

You can also help by hosting a TAPA FSR or TSR training event in 2019. Any location in the region would be considered for groups of up to 25 people, with the emphasis on venues in the Netherlands, UK, Germany, France, Italy and Spain.

Contact us via info@tapaemea.org to offer your support or to find out more.

WANT TO SHARE YOUR EXPERTISE?

Vigilant e-magazine is now circulated to the global TAPA Family in the AMERICAS, ASIA PACIFC and EMEA regions. If there's a specific topic you'd like to read about or if you have an interesting case study or feature article idea, we want to hear from you. You can contact the editor via info@tapaemea.org

KEEPING SUPPLY CHAINS SECURE

TAPA
Transported Asset Protection Association