

Container security: A multi-billion dollar cash cow ?

*Telematics Update's **Thomas Hallauer** talks to Thales and ZOCA about the lack of standards in the container security industry.*

Cargo security is a multi-billion dollar industry, with service providers who can offer efficient security and shipment visibility doing so at premium rates.

Technology providers are beginning to recoup the mountains of money they poured into R&D in response to the global paranoia and consequent demand for foolproof cargo security systems that was the world's knee-jerk reaction to 9/11.

The Homeland Security Research Corporation (HSRC) forecasts that \$12 billion will be spent on maritime container fleet security between 2006 and 2012, by which time the maritime smart container industry is expected to hit \$4 billion.

According to DeGeneste & Sullivan, ocean transportation accounts for just 8% of the total direct value of global cargo theft, followed by rail (4%) and air (1%). The biggest problem area is road transportation (87%).

While the importance of RFID and EPC technologies is acknowledged, the cost of hardware, software and integration is still an obstacle to widespread implementation.

The RFID market is set to reach \$2.8 billion by 2009, with the number of RFID tags in use expected to exceed 25.5 billion. More than a quarter of these will be active RFID tags, according to research by UK consultancy, IDTechEx.

However, the standards issue continues to rear its ugly head. No government department – specifically the Dept. of Homeland Security (DHS) in the US – has come out and given an indication of the requirement for the global container trade to use a particular technology or service. The DHS is not expected to dictate or recommend a particular technology, but rather it will suggest that all products use an open standard.

But to date there is no ratified ISO standard for technology firms to work to. But by the third quarter of this year, the industry expects a couple of standards to be announced. One is an ISO standard for electronic e-seals worked on by most of the industry; the second is a secure container device standard from a GE-led industry consortium.

Michael Naylor, technical manager at Thales Research & Technology (UK), comments: "Currently there are no standards in this area, except for the basic

ISO electronic seal standards. Niche markets and pilot trials will be able to use proprietary systems, but until we have agreed worldwide open standards the larger market will not grow. The US in particular has a desire to mandate the use of container security technology as it becomes mature, but it's hard to see how this can happen without open standards."

Jaap van den Hoek, director of ZOCA Container Security which is sponsoring the [Container Tracking and Security Show](#) in Dubai, believes that the technology providers and the market should collaborate on the development and implementation of industry-driven and supported standards, so that neither governments nor other authorities have to dictate these requirements.

Secondly, there's a tide of change from certain ranks of the industry – even from those with no financial interest in the standards debate – that the key factor for growth of container security and tracking technology and solution is a factor that lies adjacent to the technology and services: information visibility and transparency across all levels of the supply chain.

The thinking here is that, however good the container security might be, you can't leverage meaning for the container industry without the whole bigger picture, and that includes the complete enhanced solution.

"There's a big difference between the basic ISO 18185 e-seal standard and the secure container device standards," says Naylor. "I think that the ISO standard will be adopted as a first generation, to be replaced by a second generation standard such as SECCONDD or the ICSO proposed standard. There will be several different proposals. It is possible for systems to cope with multiple standards just like in DVD players, but it's more expensive and complicated. However there has to be certain common data, otherwise how can it all be used sensibly? I think we have to get the various players together to see if there is any common ground. We know the content of the proposed SECCONDD standard because we designed it, but we have not yet seen the ICSO proposal, so it remains to be seen how they could be merged into a common standard. I think that, as with the e-seal standard, there will be reluctance to change existing proprietary approaches, so reaching an agreement will take a lot of time and effort."

In respect of C-TPAT, AEO and the "secure freight initiative", Naylor says the World Customs Organisation (WCO) has agreed a set of data to be transferred. Any data received from secure containers will be in addition to this, and will not replace it, and it will be used to enhance the risk assessment information used by customs authorities.

Van den Hoek says all these initiatives leave room for interpretation, which leads to confusion. According to the AEO criteria, all expect 'an appropriate record of compliance with customs requirements'. The only difference between this and C-TPAT and SFI is the wording.

Naylor says that careful consideration is needed as to which technology side will get the upper hand.

“The market is still very much in development, and while calling for an industry standard is good, first there should be more experience with the application of a lot of these systems and services. An ISO standard would also have the preference as national or single technology (group) proposals will also cause much reaction from opposite sources.”

The last few years has seen a huge debate about what container security and tracking should be about, and it may take another five years ... if ever ... for any technology to be singled out and proved broadly successful.

In terms of the investment needed – the player who invests in the management system is not necessarily going to be the one to benefit from it. So, who’s going to invest first?

According to Naylor, the cargo consignor and consignee have the most to gain from supply chain visibility solutions. If security also provides protection against losses from theft or damage, then it’s also reasonable to expect reduced insurance premiums in the longer term, and this is where major savings could be achieved.

He believes that carriers and port operators are unlikely to invest initially, unless mandated by government. However, if it can be shown that using such systems can improve their business processes, then they may ultimately invest in them.

Van den Hoek feels that the benefits should flow back to the investor – the manufacturers and shippers, the ones who run the risk and get the blows if cargo goes astray.

He points out that missing cargo doesn’t only mean loss of profit, but also loss of manufacturing capability, order backlogs and potential damage to the corporate image. He also says that carriers and forwarders should realise that providing secure transport solutions will help them retain their customers and win new business.

In conclusion, van den Hoek says that the container and tracking market will be influenced by legislation from various authorities worldwide, as well as the outcome of discussions around mutual recognition of C-TPAT and AEO, the results of full container scanning trials and the announced Container Security Device requirements from the US DHS. It’s therefore necessary for various governments and organisations to make clear what is to be expected and how it should be implemented.

The companies that will have to work with these requirements are really waiting for services that will enable them to control the level of information, integrity and security that they need on a day-to-day basis.

The rest is about compliance.

Both Jaap van den Hoek and Michael Naylor will be speaking at the [Container Tracking & Security conference in Dubai on the 7-8 November](#). This two-day event is the place to meet top level industry players as well as the decision makers involved in policies, standards and global implementation. Get more info, reports and white papers on the subject [here](#)