

Securing the supply chain

Where is the supply chain vulnerable? What threats should we be looking for? And how can we combat these? *Digital Ship's* recent conference on container shipping security explored these issues. By Jayde Card

DIGITAL SHIP held a conference entitled "Improving container shipping security" at the Rotterdam Hilton, February 4-5, 2003.

The conference was designed to bring container shipping and supply chain professionals and authorities together to discuss and debate the issues surrounding legislative requirements, technologies to improve security in container shipping, and the costs involved.

Given the contention surrounding current security legislation and initiatives, it was not surprising that delegates representing the various parties involved had different opinions on how things should be done.

Debate ensued on various topics including the validity of various threats, whereabouts in the supply chain security plans should focus for best results, and where does the responsibility lie?

Still, there were several points of consensus; speakers and delegates agreed that the industry needs to work in co-operation with common standards in order for the implementation of security plans to be successful.

Conference attendees also agreed that there is a definite need for the formulation of contingency plans that identify risk and prepare the industry for effective threat management.

The threat

Moderator Tim Power set the scene for the day with an example of what could happen if "dirty bombs" were found in American ports.

Late last year global management and technology consulting firm Booz Allen Hamilton sponsored a "Port Security War Game" aiming to assess America's vulnerability through its ports.

The two day simulation involving 85 leaders from a range of government and industry organisations revealed that dramatic consequences could result from this scenario; every port in the US was closed for eight days; a backlog of container traffic ensued that took 92 days to clear; the DOW dropped by 500 points; the event cost the US economy \$58 billion in revenue, with economies of trading partners also affected. Mr Power stressed "This is not a fantasy, this could happen."

Security as it was once known is changing. Dick McCormick, Vice President of Pinkerton's Business Risk International commented, "Once we only had to keep things from leaving containers, now we have to keep things from being put in."

The exception to this is the narcotics trade, but Mr Power pointed out that it is the nuke in a box that holds the public imagination and that of the industry.

Earlier this year UK television compa-

ny BBC reported that a dirty bomb was "one frightening possibility", following the release of a terror warning from the UK Home Office.

Later toned down to reflect a more general warning and need for vigilance, the Home Office statement originally cautioned, "Maybe they [terrorists] will try to develop a so-called dirty bomb, or some kind of gas; maybe they will try to use boats or trains, rather than planes."

Weapons of Mass Destruction

David Hopps of Tag 24, a security company that specialises in the protection of client's products and intellectual property rights, noted that the term "weapons of mass destruction" had been said 27 times, and then asked, but did we know what a WMD actually is?

Do those appointed with the task of conducting security checks know what to look for?

There are four main categories of WMD



Damian Viccars, UK Freight Transport Association

conventional; nuclear; biological; and chemical.

The so called "dirty bomb" falls under the category of nuclear WMDs, consisting of a conventional bomb surrounded by radioactive material. When the bomb explodes, millions of radioactive particles, some the size of dust, scatter over a wide area. Until every single piece is collected the whole area has to be kept clear of people and can have disastrous consequences if allowed to contaminate a population.

So, how is a terrorist likely to use these? Mr Hopps suggested there was no definitive answer to this question because there are so many variables, instead risk assessments ought to be carried out and contingency plans devised.

Sam Ignarski of Wavelength, a facility for managing insurance of ports and ter-

minals, questioned the validity of focusing on one threat in particular, asking, "Is this security or the illusion of security?"

His suggestion that the "bomb in the box is a rather improbable risk" was met with cries of controversy from the audience, many of whom believed the threat a serious one.

Still, Mr Ignarski suggested that security plans should not focus on one threat, but rather should tackle such risks in combination with other initiatives, e.g. anti-smuggling and anti-drug operations. "It all fits better when it has some primary and secondary purposes," he said.

Responses

There was agreement that proper contingency plans do not exist within the industry. In reference to what would happen should a WMD be found in a container, Mr Power commented, "I don't think anybody has thought it through."

"The consequences of port closures aren't understood," he added.

Similarly contingency plans for removing problem containers are mostly non-existent, noted Dennis Mike Egan, head of Homeland Security with US consultancy System Planning Corporation, who introduced the idea of the "penalty box", a place to keep dangerous containers and deal with risk away from ships and ports.

Mr Hopps suggested that the industry needs to analyse a range of scenarios to enable senior management to hone their decision making and ensure that a graduated response follows any threat, guided by whether the threat is perceived as low medium or high.

Mr Hopps remarked that terrorists can close a country down just by threatening, and in this way a graduated response will go a long way in ensuring that the business isn't more crippled than it needs to be.

Security Initiatives

Damian Viccars of Freight Transport Association (FTA), suggested that the industry needs to plan ahead and avoid new requirements being sprung upon shippers.

The FTA believes that a system of known operators and shippers is required, similar to that which occurs for UK air freight, requiring registration and preparation of a shipper/operator security plan (SSP/OSP) that "demonstrates to customs and security forces that appropriate security measures are in place that cover premises and day to day operations that secure and prevent infiltration by terrorists and their material."

Or "alternatively a shipper may have his consignments made secure by a freight forwarder who has been officially recognised as competent to perform this role."

For more information see <http://www.fta.co.uk/information/otherissues/security/index.htm>

IMO

Ports security has come into focus since 9-11, said Peter Zint, of Hamburg Port Consulting, with an "overnight security inclusion" to the International Maritime Organisation's (IMO) regulations.

The IMO's amendments to chapter 11; some compulsory, some only recommendations, saw the call for a mandatory port facility (i.e. the ship-port interface, not the entire port) security assessment and plan. These changes are to be implemented by July 2004, although Mr Zint posited, "My



Sam Ignarski of Wavelength Insurance, author of the popular Bow Wave newsletter

personal feeling is that things will still move a little bit slower. More realistic is that assessments [only] will be done by July 2004."

The purpose of the risk assessment is to identify the threats and weaknesses, and then prioritise measures to reduce vulnerability said Mr Zint. In addition, ports are required to devise a procedural plan, which includes knowing how to contact relevant authorities.

The security plan is based on the assessment and can be developed by the port security officer. This then introduces the issue of training remarked Mr Zint, for ports staff have no experience of port security besides current anti-theft initiatives.

According to Mr Zint, the risk assessment process is still rather elusive. He posited that ports can only address vulnerabilities that have been detected, but how far do you have to go in identifying risk?

Mr McCormick commented, "You must look at the worse case scenario if only to decide that there isn't anything you can do about it."

Airways

John Edwards, head of security with British Airways World Cargo, told conference attendees that BA has endured high threat levels following 9-11, with Britain a known terrorist target and the airway being so identifiably British. Mr Edwards remarked it is clear that there is no option but to focus on security issues.

Mr Edwards noted the importance of "a cohesive management system" when implementing a security plan.

"People at the top of the organisation must believe in ensuring security... it should be your *raison d'être*," he said.

CONTAINERS & SECURITY



Left to right: John Edwards, network safety and compliance Manager, British Airways World Cargo; Dick McCormick, VP business risk international, Pinkertons; David Hopps, head of physical security and crisis management, Tag 24; Tim Power, Power Project Resources (moderator) and Peter Zint, Hamburg Port Consultancy

Companies need to invest in terms of time and people, i.e. ensuring they have the right skills and training, and equipment.

The need to test and revise contingency plans was emphasised. "It's a mistake to believe then that that's the job done. You need to not only put [a security plan] in place but also make sure that it is operated effectively," said Mr Edwards.

"Providing you have your house in order there is a very good chance that any terrorist attack or attempt at a terrorist attack will go somewhere else," posited Mr Hopps.

Collaboration

The need for co-operation and collaboration was echoed throughout the conference.

"Terrorists collaborate and so must we," said Mr Edwards. "Security is not about competition."

"In order to deal with a crimes syndicate then we must become equivalent to the syndicate ourselves," added Mr McCormick.

Still, effective co-operation requires a uniform approach across countries and organisations and in this way the design and implementation of satisfactory standards is essential.

The need for intelligence was one reason for co-operation between various countries and organisations.

Launched in May 2002, Eurowatch is an example of collaboration across organisations and countries. Peter Vyvyan-robin-

son, of TRI-MEX and originator of the concept for Eurowatch, claimed the initiative was the "missing piece of the puzzle."

Approximately 800,000 commercial vehicles and cargoes are stolen annually in Europe. When a vehicle carrying cargo is stolen, Eurowatch integrates vehicle GPS data, which would ordinarily only go to authorities in the country of origin, and web technology to provide data to accredited national service providers, including local police.

Thus far Eurowatch has recovered all vehicles reported to the service.

The service includes all countries in Europe except Greece, and will be extending its reach this year. Eurowatch membership costs EUR250 per vehicle per year.

Responsibility?

The issue of responsibility rose during discussion. Mr Zint believed there was a "problem of whose job is what" and therefore where responsibility lies. Responsibility for security is also somewhat dependent on where in the supply chain security plans focus.

Mr Edwards suggested that key to an effective security operation are the first points of uplift. He suggested that watching these points can reduce the burden down the supply chain.

Mr Ignarski questioned "to what extent it helps to get a good grip on those sorts of places [like port of Rotterdam]."

He believed it is "largely sterile to submit

a sufficiently well run facility to added measures when the source of the problem is in the shadowland," and suggested that security operations should inspect up country rather than down near the port gate.

In terms of cost, Mr Viccars suggested, "We are not the first line of defence but could act as a second net and instil confidence," adding that if we are doing the job of the department of security this should be a factor in who pays the costs of conducting security initiatives.

Technology

Technology was seen as having an important role to play in combating crime and the bomb in a box threat, particularly when used in correspondence with collaborative initiatives.

Mr McCormick commented, "Technology becomes much more important when everyone's all talking to each other, that way it becomes more effective... that's what will stop weapons of mass destruction, biological warfare, dirty bombs."

One example of these initiatives is Smart and Secure Trade Lanes, in which electronic tags, e-seals, are placed on the outside of all containers originating from participant ports as a means of increasing security.

These tags store information such as contents, route travelled and destination.

"War is about pitting your supply chain against that of your enemies," said Mark McClade of Savi technology, a founder of the scheme.

Karl Bohman of AllSet Tracking claimed that e-seals offered the industry a more secure and cheaper alternative to mechanical seals.

Mr Bohman disputed claims that e-seals were uneconomical, positing that permanent re-usable seals provided an economical alternative to disposable e-seals, however, acknowledging scepticism exists, Mr Bohman lamented that the value of e-seals will not be seen until satisfactory security protocol is established and frequency issues are resolved, allowing for a global solution and infrastructure.

Another technology proving useful for supply chain security purposes is SAIC's VACIS (vehicle and cargo inspection system) providing scanning technology in various forms for inspecting vehicles and containers.

Victor Orphan of SAIC, claimed that the systems had proved very useful to customs authorities globally, exemplifying Malaysian customs, whose revenue increased by \$158 million after four months of using VACIS, with the systems paying for themselves after a week.

Data

Increased co-operation between authorities and organisations will inevitably lead to increased information, which needs to be managed effectively.

UK based Autonomy is one company aiding the management of information. Autonomy provides software that uses algorithms to determine what information is most important in a file and categorises the information accordingly.

The system can incorporate information from television and telephone (for which the audio needs to be transcribed), word documents, databases and email.

Kenneth Donau, of Autonomy, said that after analysing patterns, the software will alert the right people to discoveries so that they can determine necessary action.

The implementation of new security initiatives will also require effective management of information. Ashley Skaanild of GT Nexus commented that carriers are going to be incredibly busy inputting data received largely manually and are going to be asking customers to send information way before the vessel loading dates in order to comply with the new 24 hour rule.

According to Mr Skaanild, GT Nexus' acts "just like a telephone line" providing a direct line from shipper to carrier, who are not charging for bill of lading should it come on time and electronically.

In addition, through time stamping, GT Nexus can provide better control and management of information. DS

Should US customs inspectors be present in European ports?

"We say, 'if you want to play with us, here are the criteria.'" - Bryan Evans III, customs attaché to the Port of Rotterdam

"Very soon we will have to decide if we continue to operate our cooperation to the US, or try to find our own way, but concentrating on imports, not exports"

- Alexander Wiedow, European Union director of Customs policy

Digital Ship's Rotterdam conference in container shipping security last week included some interesting debate about the presence of US customs inspectors in European ports, in particular Rotterdam.

The Americans argue that they need to do something to improve the security of container shipments into the US, it is much easier to do this at export ports rather than in the US, they looked for partners willing to co-operate and the Port of Rotterdam agreed to let US customs inspectors into the port.

The European Union argues that the Americans should have worked together with European customs and developed a program to share information in both directions, rather than just installing their own inspectors alongside the European ones, asking the Europeans for data and not giving data to the Europeans in return.

As has been widely reported, the EU has started infringement procedures against countries in Europe which allow US customs inspectors, saying that it believes this goes against the European constitution, and causes more disruption than benefit.

Furthermore, if the US does not go for a more reciprocal approach towards inspections the EU will stop cooperating with them, and develop its own system, more geared around imports into Europe rather than exports from it.

The European Union is not arguing for the whole world to be involved in agreeing on a common system for evaluating

the risks of containers and the information which should be shared, because this will take too much time. However it is arguing that the US and EU should sit down together and agree on a policy, rather than the US working with individual ports and

nations within the EU.

Some industry observers say that the US has been the first to make an effort with its Container Security Initiative and the EU should be aiming to work with this, rather than asking the US to start

Alexander Wiedow, director, European Commission Taxation and Customs Directorate, assisted by Jozef.Hupperetz, also of the European Commission





Left to right: Bryan Evans, US Customs Attaché to the Port of Rotterdam; Mark McGlade, managing director Europe, Middle East and Africa, Savi; Captain Mike Egan, director of US homeland security for intermodal transportation, System Planning Corporation; Ashley Skannild, regional director, GT Nexus; Alexander Wiedow, director, European Commission Taxation and Customs Directorate; and Tim Power (moderator)

again from scratch, with the eventual aim of a fully reciprocal system.

Bryan Evans III

Bryan Evans III, US customs attaché to the Port of Rotterdam, acknowledges that the Americans cannot solve the problem of improving container shipping security by themselves.

"We recognise that the trade community has to be positive with us," he says. "But we say, if you want to play with us, here are the criteria."

"We have to do our job as a customs services." If you have a ship you want some level of confidence that what's on the ship is not going to go boom.

"Carriers said, that makes a lot of sense. There must be something good about the program because people are signing on."

"Making sure that trade is not impeded is very important, he said. "If we inspect in the port, we normally get in an inspection when it's sitting in dead time. Most containers arrive at the terminal 72 hours before the ship goes."

The 24 hour rule, saying that all containers must declare their manifests before the ship sails, in fact puts a lot of pressure on US customs because they have only 24 hours to decide whether or not to allow a particular container onto the vessel. "It keeps up our promise that this is not going to alter trade," he says.

Alexander Wiedow

Alexander Wiedow, director for Customs Policy with the European Union, argued that the system is not very balanced between the US and EU.

"Commissioner Bonner [architect of the US container security initiative] says, 'our first objective is to protect the US citizens'," he pointed out.

Mr Wiedow observed that the US customs is asking European customs officials for advice if they are suspicious about a particular container, which costs money to provide, although intelligence is not being made available from the US to European Customs in the same way.

"We would expect some beneficiaries from carrying out these controls," he said. "It is generating a lot of costs."

"We don't object to the 24 hour rules as an intermediary check," he said. "But [long term] sharing the responsibility and burden is the only way to manage the situation."

"Very soon we will have to decide if we continue to operate our cooperation to the US, or try to find our own way, but concentrating on imports, not exports."

The port of origin

Mr Wiedow pointed out that with 80 to 90 per cent of containers in Rotterdam originating from outside of Europe, it made far more sense that the container should be examined in the country where it was originally loaded, not a transit port.

Mr Wiedow agreed that customs is the right agency to take responsibility for container security in the transit chain, filtering out the dangerous cargoes, being the first point of contact for the container and getting to know the shippers involved in their geographic region.

But this only works if the customs agency is physically located in the country of container origin.

Standards

Standards are gradually being developed for electronic communication between customs, deciding which data should be collected and which should be exchanged, and this would create international trade with a much more flexible approach to customs.

Customs agencies all over the world, of course, ask for exactly the same information from shippers, the 14 fields on the

manifest form; where they differ is what they do with the data and the terminology they use.

The suggestion is that US customs officials sit down with the EU as a whole, quickly work out a program for exchange of customs data between them, which can be rolled out in all EU member states and then the rest of the world.

Mr Wiedow agreed that creating international agreement would take a lot of time, and letting all European member states develop their own standards would be complex.

"We need a bilateral agreement with the US," he said. "I think it will be a more standardised and harmonised approach. And we cannot afford to leave the selection down the (European) member states."

Mr Evans and Mr Wiedow were in disagreement about the current level of interest the US is showing in discussing common customs standards with the EU.

"We sent a letter [to Commissioner Bonner] in December and haven't received an answer," said Mr Wiedow. "Where are we in the discussions - we have not got very far."

"The Commission could have communicated via the G8," asserted Mr Evans III. "Commissioner Bonner has stated that he is more than willing to engage in a dialogue with the EU."

Infringement procedures

Mr Wiedow acknowledged that one of the reasons for US reluctance to sit down with the EU in this way might be the fury at the infringement procedures the EU is currently taking with member countries which have allowed the US inspectors in.

"The EU has taken up infringement procedures [against the Container Security Initiative] because we think it is creating more distortions than helping the security issue," he said.

"We have to make sure that the European constitutions are safeguarded. I think the US would act in the same way."

I understand that the US is irritated by the infringement procedure but I think they have to understand that there are issues at stake."

Speed

Mr Wiedow knocked back comments from conference delegates that the US had worked with individual European countries as the best way it could quickly achieve increased security, saying that he



Kenneth Donau, Autonomy

thought that the improvements in security could be achieved just as quickly if the US addressed the EU directly instead. "The main thrust is the testing period," he said.

"This was an issue of security," said Mr Evans III. "We looked at partners willing to cooperate and we found them."

"The task ahead of us is absolutely immense," comments Mark McGlade, head of SAVI Europe Middle East and Africa, who also participated in the discussion. "No-one knows all the answers but you have to start somewhere. The US customs initiative has to be endorsed. We need to bring our teams together."

"The EU could start a completely parallel initiative," he warned. "They should compliment the initiative, not fight it."

Data transparency

Sam Ignarski, port insurance consultant, observed that the US and EU have different approaches and laws about data transparency, and it was his observation that under freedom of information legislation in the US, it is often much easier to obtain data than in Europe. If European and US government agencies are going to exchange data then there needs to be common approach to which data to make public. **DS**



Bryan Evans III, US Customs Attaché to the Port of Rotterdam, attracts comments from the floor