

Tightening up

Security is proving costly to all parties in the maritime industry. **John Fossey** reports on the measures being implemented to ensure that ports, ships, containers, and information flows, are robust enough to prevent theft, fraud and above all a breach by potential terrorists.

There is no doubt that the world is a more dangerous place. Terrorist attacks in places such as New York, London, Madrid and Bali over the past four-and-a-half years have meant that security has become higher profile in virtually every walk of life.

This has been particularly true of international shipping. The tanker and container sectors have received the greatest attention, mainly because of their potential use by terrorists to launch further attacks.

A container on a door-to-door move, for instance, could be loaded with a weapon of mass destruction and delivered to the commercial hub and/or seat of government of any major city in the world. Or terrorists could target ships on specific trades, interrupting the global supply chain, causing untold damage to economies and heightening political instability.

Against this backdrop, the US Government and a host of international bodies, such as the International Maritime Organisation (IMO), General Chamber of Shipping, World Customs Organization and Unctad, have worked tirelessly on how the international transport chain can be made more secure.

Maritime-wise, the most important initiative was the introduction of the ISPS code in July 2004. But there have been a raft of other measures introduced since that first terrorist attack on the World Trade Center towers in New York City on September 11, 2001, including:

- Customs-Trade Partnership Against Terrorism (C-TPAT)
- Container Security Initiative – geared to foreign ports handling cargo destined for the US and where US Customs officials are allowed to inspect goods
- 24-hour cargo manifests
- use of electronic seals.

The C-TPAT programme has achieved only limited success – question marks remain over the validation and ongoing verification programmes that actually determine whether or not members' supply chains are secure. It is understood that, as of autumn 2005, less than 15% of companies that had signed up for the C-TPAT initiative have been validated, and developments to the programme had been slow to materialise.

Meanwhile, and in sharp contrast, there has been considerable expansion of the US'

Customs Border Protection (CBP) agency's CSI programme. It now covers 42 ports, with Lisbon (Portugal) the latest to sign up in December 2005. The programme is well on target to have 50 ports signed up by the end of 2006, allowing about 90% of all transatlantic and transpacific inbound cargo flows into the US to be pre-screened.

Arguably, though, the US Government believes that still greater protection is needed. In November, Michael Jackson, Deputy Secretary of Homeland Security (DHS), said the next generation security system would need to be a 'fundamental philosophical jump from that of today'.

He elaborated: 'Cargo security will not work if each country tries to set up separate security regimes using disparate information technology systems and tries to secure shipments through a series of unrelated bilateral arrangements. The World Customs Organization's (WCO) efforts to spread standards for global trade facilitation and security is a tremendously good sign because it moves us beyond just the US Government's effort to regulate industry.'

The European Union is also tightening up its security efforts – for more details, see 'EC security proposal expected in spring', p23.

In terms of managing and collecting data, Jackson is keen that the private sector is involved and that third-party information clearing houses are set up. He said: 'We have to switch the business model to create intermediary institutions which are non-profit or for profit, which are essentially you in the middle between the actors in the supply chain and governments who need to gather information about the pre-history of a container.'

Jackson continued: 'Data from purchase orders, bookings and other early transactions would help CBP be more sophisticated in profiling which containers need to be inspected.'

A key to better security in the supply chain is to get all stakeholders to cooperate – and that means state agencies and private companies. Data that supports the physical move-

ment of cargo can also become corrupted, and vigilance and supervision are needed at this level, too.

In addition, there is the whole issue of trade compliance (see 'Policing trade').

The US Government is now into phase three of its Operation Safe Commerce programme, a key part of which is C-TPAT Plus. The latter includes research into new and more sophisticated container security and monitoring devices, and the so-called smart box concept (see 'The first line of defence', pp67-69).

IBM Consulting Services (IBMCS) has become heavily involved in the security issue, having worked on separate projects in conjunction with Maersk Logistics and the US DHS. According to Stefan Reidy, leader of IBMCS' so-called Intelligent Trade Lane initiative, the intention 'is to bring real-time visibility to the global supply chain by improving the quality of container tracking and increasing the security of goods being transported.'

The project has involved fitting wireless-based tamper-resistant embedded controllers (TRECs) into freight containers. These devices automatically collect information on aspects such as location, conditions inside the container, as well as any intrusions. Such data from the devices are fed into a non-proprietary sensor network and business integration system, enabling participants in the supply chain to readily access the information.

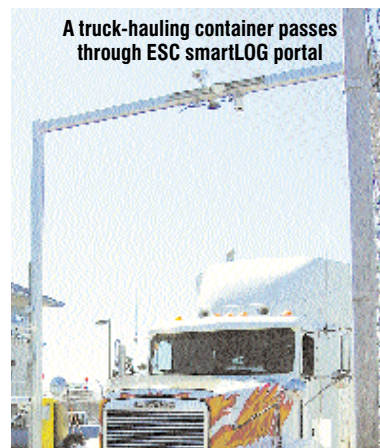
According to Reidy, the information can be connected to decentralised databases so each participant is seen to have ownership of the content. Equally, though, networking allows users to share information.

At the launch of IBMCS' secure tradelane programme, which comprises a part of the company's more embracing Global Movement Management programme, Mogens Roedbro, a partner and vice president of IBMCS, said: 'Our objective is to enable globally integrated business by capitalising on the information generated during the tracking process, and at the same

time improve the security of the operation.'

The project is still being tested, with a significant commercial pilot programme scheduled to take place in March 2006. Full implementation is expected in the second half of 2006.

According to several independent observers and participants in the



freight transport sectors, the IBM/Maersk Logistics initiative offers real opportunities.

James Rice, director of the Integrated Supply Chain Management programme at Massachusetts Institute of Technology, said: 'The ability of this project to create an environment where all supply chain participants have real-time visibility while also leveraging industry standards will eliminate some of the complexity from the operation. It also offers a promising approach for a more truly resilient and secure transborder supply chain.'

Reidy added: 'It also helps improve customers' stock management programmes, thereby effectively pricing their goods on real-time supply information. Additionally, insurers can determine if and where losses occurred.'

Tracking and securing containers is only one element in the transport chain. What about the ships, for instance? A number of long-range monitoring devices are available, including ShipLoc, which was developed by CLS, a subsidiary of the French space agency. This can plot a ship's position up to 24 times a day, with the information being relayed to a dedicated website.

Clearly, there is a need for a long-range ship identification and tracking system to be implemented, and, while the US Government had offered to fast track and fund this, other coun-

tries opposed the plan. The consensus now is that this will be achieved through the IMO.

In Australia, the government is spending heavily – approximately AUD150 (USD113) million – on securing its maritime sector. Over the next two years, the nation will introduce its Maritime Security Identification Card system (MSIC), which is tailored to employees and service providers (such as maintenance contractors) in marine facilities, aboard ships and off-shore gas/oil installations, and an e-visa system for visiting seafarers. The MSIC programme will become mandatory in January 2007.

Of course, enhanced security means higher costs to all parties engaged in the supply chain, and it has led to arguments over who should pay for it and how much should be subsidised by governments. After all, a more robust and secure supply chain is in the interests of both international and national security. Where surcharges and/or additional premiums have been levied, whether by port authorities/terminal operators on ocean carriers or shippers directly or the liner

companies on their customers, intense debates over transparency have emerged.

Companies engaged in liner shipping generally do not trust each other, with shippers/consignees viewing most surcharges as revenue-enhancing devices rather than cost recovery measures. Meanwhile, carriers accuse ports/terminals of profiteering from security, believing that charges should be a one-off and not levied annually.

Perhaps there is a misunderstanding here of the need and the associated costs involved in maintaining and upgrading sophisticated computer and surveillance equipment, perimeter fencing, scanning equipment, employment of security personnel and so on.

The use of gamma-ray cargo inspection machines in ports has become more widespread and the number of containers inspected has generally been stepped up, although this varies on a country-by-country basis.

Although stricter measures have seen increased seizures of illicit material, especially drugs, and prevented the evasion of millions of dollars of tax revenues, the supply chain for importers/exporters has lengthened and it is now more challenging for service providers to meet their just-in-time and guaranteed delivery time assurances.

POLICING TRADE

Trade compliance issues are gaining significance and the US-headquartered Bureau of Industry and Security (BIS) is tightening up and ensuring good practice in the export business. BIS is especially keen to stamp out illegal exports, in particular preventing the movement of weapons of mass destruction and goods that could easily be diverted for military use.

In 2005, more than 30 criminal convictions and 60 civil actions were taken by the agency, this raising USD7.7 million and USD6.8 million in fines respectively.

Several companies offer trade management solutions software, with NextLinX, which was recently acquired by East Rutherford (NJ)-based Management Dynamics (MD), the largest in the sector.

'We have invested substantially in our software since the company was set up in 1994 and we have staff that have been involved since the start,' explained Rajiv Uppal, who was the founder and chief executive officer of NextLinX and now fulfils the role of chief software architect at MD. 'It means that our automated solutions are capable of handling the most complex of trading issues, even for the very largest corporations. At the same time our systems ensure full regulatory compliance with Customs authorities and initiatives, such as those introduced by agencies such as the US Department of Homeland Security.'

Uppal singled out its recent Restricted Party Screening (RPS) service. Targeted at small and medium-sized enterprises trading in the US, it allows importers/exporters to send MD their customer lists, which can then be screened

against all official denied persons lists.

'RPS allows full compliance with, for example, the US Patriot Act,' said Uppal. 'With smaller companies' limited resources but desire to get more involved in international trade, RPS provides them with a cost-effective solution that ensures full compliance with the rising number and increasingly complex nature of government and security regulations. I see this product as having significant growth prospects.'

Uppal said MD had modules covering import, export and preferential trade agreements, and has also developed a specialist web-based information/advisory service called Trade services.

'It is our intention to assist companies to trade effortlessly and honestly in the hope that fines, penalties, any suspension of trading privileges, and so on, can be avoided,' he said. 'It should always be borne in mind that importing and exporting is not a right but a privilege.'

'With more rigorous checks in place, there is a much higher level of companies getting caught, perhaps as high as 5% and we can reduce this ten-fold to just 0.5%. In addition, there is a clear tendency for authorities to take a more lenient view on those businesses that have made every effort to put in place practices aimed at preventing fraud and other malpractices.'

MD's trade management and solutions database houses up-to-date trade content and business rules for about 120 countries and enables companies to fully automate their import and export processes.



Rajiv Uppal, Management Dynamics