Port security – beyond the ISPS code

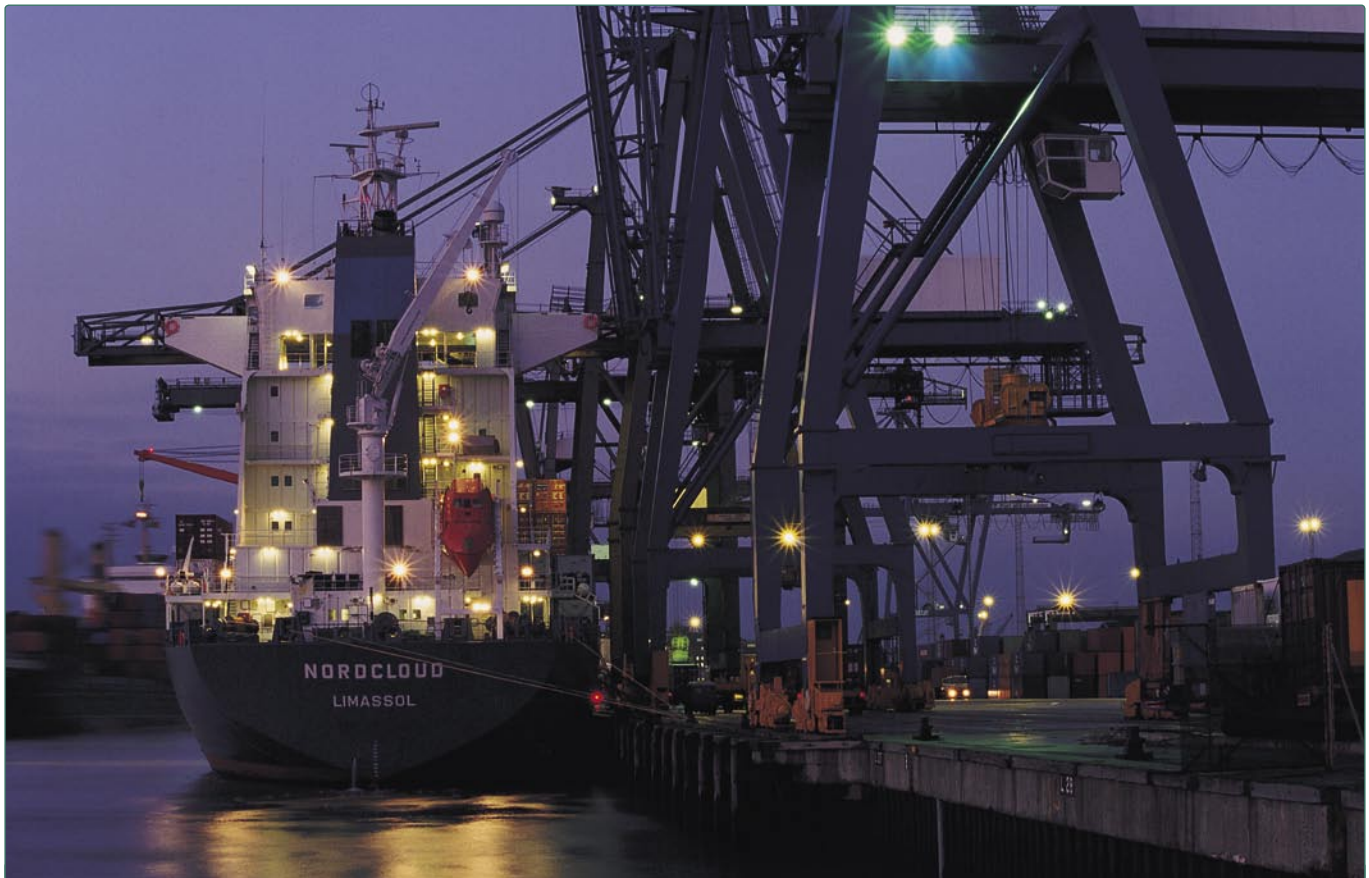
Lloyd's Register Quality Assurance Ltd., London, UK

Since 9/11, port facilities and ships have been identified as the primary potential threat to international security. The theory behind this seemed to suggest that ships and their port interfaces were vulnerable to threats and were the means by which international terrorism would be able to perpetrate their deeds. The more cynical in the industry suggested that ships and ports were selected because they were easy to ring fence and there was an established mechanism in place to introduce regulatory requirements; through the IMO. Thus, the International Ship and Port Facility Security (ISPS) code was created, and by July 2004, some 35,000 ships were certified compliant with the ISPS code and deemed 'secure' and the world was a safer place. Or was it?

Visit any port and look at what security arrangements are in place. Some have three metre high boundary fences, some don't. Some have cameras peering into every corner; some rely on just a few or none at all. Some have guards patrolling and static guarding at gates and entrances and exits, some don't or, if they do, the guards are not always instructed on what to look out for. So what should ports be doing to protect ships taking on or discharging cargo and passengers, and the supply chain with which they interface? How can a port authority judge what should be done to make itself and its supply chain partners secure without overdoing it or spending unnecessarily on infrastructure, equipment and resources? The decision making has to be part of an intelligent process; top management led that adopts a – 'what if?' approach and linked to a – 'what should we do?' Such a process is generically called risk assessment or risk management. The ISPS code recognises that the Port Facility Security Plan (PFSP) is 'fundamentally a risk analysis of all aspects of a port facility's operation to determine susceptibility to attack.' Risk assessments needs to consider all sources of risk, such as security threats or events that might interrupt operations and then assess the likelihood or vulnerability and consequence of each of these occurring. The result will be a documented record of all potential events, not just those considered possible or probable, but all, so that all those thought of during previous iterations can be revisited periodically for re-evaluation.

Evaluating risk

Evaluating risk for all eventualities is not an easy process. It can't be done by one person sitting in a dark room with a blank piece of paper. It's part of the intelligent evaluative process that requires input from a 'team' of experienced, knowledgeable people who can provide the necessary cross functional and operational input about all aspects of the port facility's internal activities and external influences that might also impact on the port facility's up-stream and down-stream supply chain security. The team needs to consider every eventuality, however unlikely or 'off the wall.' To do this properly, with confidence that outputs will be treated seriously and dealt with the necessary resource and investment, top management support and commitment is needed from the outset.



Many have argued that it is not the ports themselves that are the sources of risk but perhaps the goods and containers that are transited to and from ships.

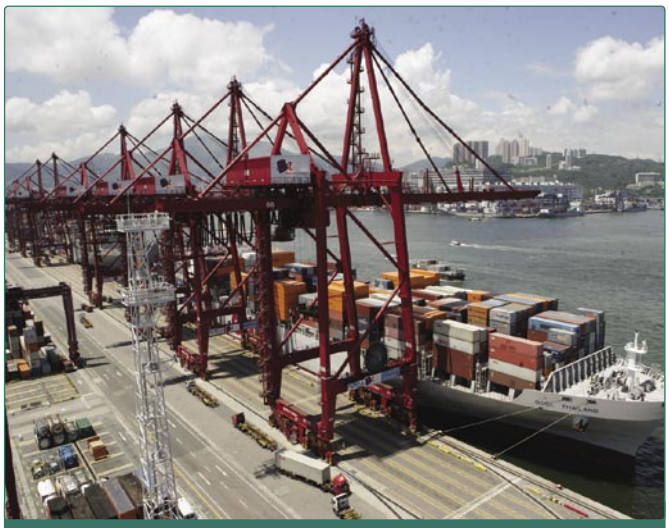
Having gone through this in-depth root and branch process, the operational arrangements that are required to mitigate the impact or reduce the likelihood, need to be put in place. This may require changes to working practices, operational instruction, training or behavioural adjustments for key staff who deal with security matters on a day to day basis.

Taking responsibility

For most ports, the risk assessment was the means of getting through the ISPS approval process, but the ISPS code was developed to deal only with what happened inside the port facility and at the ship port interface. Supply chain security, however, cannot be assured by this alone. Many argued that it was not the ports themselves that were the sources of risk but more likely goods and containers that transited to and from the ships. Should it be the responsibility of ports to make the supply chain secure by identifying and stopping terrorists' and criminals' illicit materials and booty from moving through the port and further along the supply chain? In this time of elevated security alerts it has to be the responsibility of all who provide supply chain logistics services to take the necessary steps to reduce vulnerabilities and the likelihood of events from occurring and that means controlling what is under direct management and influencing the activities of supply chain partners up and down the supply chain. Most organisations take steps to check that purchased goods meet expectations and are in accordance with the written specification. Receiving goods for onwards shipment is no different. Appropriate steps should be taken to verify that empty containers are empty and that the goods in the containers have not been tampered with since the point of departure by verifying the integrity of container seals. Other checks may be necessary as determined by the risk evaluation but these should reflect the risk and security level prevailing at the time. Doing nothing and just relying on the fact that it's been all right before is not taking security seriously and ignoring the responsibilities that must be taken on board.

C-TPAT and AEO

The port industry and its regulators are now moving beyond the ISPS code into a world of additional voluntary codes; codes such as the US Customs – Trade Partnership Against Terrorism (C-TPAT) and the European Union's Custom's Regulation for Authorised Economic Operator (AEO), both of which have been introduced to meet the World Customs Organisation's SAFE Framework of Standards. These are just two high profile schemes that nations and regions are introducing. These are voluntary so far, and national regulators have said that there is no intentions of making them compulsory, but to join the Green Lane 'club' which grants smooth uninterrupted transit of goods throughout the supply chain, adoption of these voluntary codes will become an industry expectation and a virtual 'must do.' These and other schemes for enhancing supply chain security – such as the CSI, TAPA and BASC codes, have several things in common. As already said, they need to address the supply chain wider and further up and down than does the ISPS code alone.



To ensure the smooth uninterrupted transit of goods throughout the supply chain, adoption of voluntary codes will virtually become imperative.

They also require the ISPS risk assessment to include the activities of customers, suppliers, partners and stakeholders. But fundamentally they cannot be applied successfully, consistently and effectively without an overriding top management driver being applied, which consists of systems for designing and documenting the management requirements and ensuring they are applied at all stages of operation including measuring and monitoring for effective implementation.

ISO standards

Both the US Government's Security and Accountability for Every Port (SAFE) Act 2006 and the guidance to the European Commission's AEO Regulation refer to the role that International Organization for Standardization (ISO) standards can play in helping with the implementation of the schemes for enhancing supply chain and port facility security. ISO working groups have been very active since 2005 working with industry groups and experts to develop a series of standards that describe the management arrangements for enhancing supply chain security. The ISO 28000 series of standards provide requirements for self, second or third party verification and guidance for supply chain management systems, which are now being applied by industry sectors, including ports and other logistics companies.

Compliance with these standards sets a sound framework for compliance with the voluntary governmental codes which will become, very soon, the industry norm for doing business in the international intermodal supply chain in which ports play such a pivotal role.

These are voluntary so far, and national regulators have said that there is no intentions of making them compulsory, but to join the Green Lane 'club' which grants smooth uninterrupted transit of goods throughout the supply chain, adoption of these voluntary codes will become an industry expectation and a virtual 'must do.'

ABOUT THE COMPANY

Lloyd's Register Quality Assurance Ltd. (LRQA) offer a number of services including assessing companies security performance, certifying supply chain management systems and training security management personnel.

ENQUIRIES

Lloyd's Register Quality Assurance Ltd.
Email: enquiries@lrqa.com
Website: www.lrqa.com