

# ISPS and security systems technology

**Michael Fairnie**, Principal Consultant Maritime, Olive Group

This period of prolonged economic downturn has affected the movement of goods greatly, not to mention the movers of these goods and associated service providers. They face a prolonged battle against falling revenues and Capital Expenditure reductions whilst jealously guarding Operating Expenditure and apportioning it more to core revenue generating uses (quite correctly so).

## Saving money

We at Olive Group feel that it is the right time to reiterate the potential revenue savings available to Operators within the commercial maritime domain if they were more aware of how the ISPS process can be applied to better suit their needs both from a security and a fiscal perspective.

When the good times are rolling it is relatively easy, or at least easier than in present times, to specify or have specified to us a wide range of technologies for implementation and use within a port security system. However, when we are in a downturn period, everything must be justified in depth and to the highest degree. Nothing wrong there I hear you say, and I would agree.

We must attempt to make better sense of the sometimes ambiguous relationship which exists between the regulatory compliance regime existent within most ports and the utilisation of costly technology.

## Overcoming obstacles

Common objections to ISPS that are often heard include: 'ISPS does not tell us specifically what technology to install, so how does it help us' or 'we want cameras but we do not want an assessment, that is a waste of time and money'. The most difficult obstacle to resolve in the client's best interest goes something like 'we have a new port, it will have or has xxx security cameras, a control facility, x type of access control located at x, y and z etc. but now we need it all to be ISPS compliant'.

## Risk assessment

This tells us many things and poses more than a few questions, not least that possibly the process of assessing threat, hazard and risk etc. has not been conducted at the correct time or indeed at all. So if it has not, how has the identification of critical assets

been conducted, and following logically on from this, has the need for countermeasures or mitigating actions been realised.

This leads us to the most crucial questions of all. Do we know if we are protecting the correct areas, assets and resources effectively? Cost to benefit ratio – is it right, or are we wasting money? I need go no further, as I am sure that you appreciate the point I am making.

So the ISPS code is partly an assessment tool, which if even just followed chronologically, can allow business managers pre-planning opportunities in order to make informed decisions as to the most operationally and financially effective deployment of sometimes expensive technology. It even forces the development of a set of 'Key Performance Indicators' for good measure, which if correctly applied, assist in continually keeping costs down and utilisation up, a win/win scenario surely.

## ROI

Implementation of security technology is often perceived to be a sunk cost after spend, however an effective assessment can go some way to change this perception. Additionally a well thought out and intelligent planning process, if functionally appropriate, can help to maintain predetermined Return on Investment (ROI) levels over longer terms.

## Interpretation and applications

Therefore, the ability to interpret the requirements of the ISPS code correctly and apply them proficiently should no longer be solely considered and confined within the relatively narrow context of security. If we can read between the lines, we will find many helpful tools which aid decision makers to spend wisely on technology, gain a solid understanding of the framework and the advantages to commerce within, and disseminate this knowledge throughout all levels of the business.

We understand that what we do for our clients could not be described as being core business activity but we can save investment dollars and seek proper utilisation of these costs over a protracted period. In effect we can save money and that is never, ever a bad thing.

Indeed we follow this ethos whilst providing our services to some of the largest players within the industry. We know they appreciate it, they tell us so.

### ABOUT THE COMPANY

Olive Group is an industry leader in security and risk management, operating globally through its Headquarters in Dubai and regional offices throughout the Middle East, Europe, North America, Africa and Asia. The company specialises in risk management, technology systems design and integration, business continuity planning, crisis management, training and implementation of security master plans to commercial, industrial and Government clients.

### ENQUIRIES

Web: [www.olivegroup.com](http://www.olivegroup.com)