Intelligent security planning for ports

Liam Anderstrem, Business Development Director, Olive Group

The threat from major terrorist attacks is very real for port operators and those responsible for ensuring the safety and security of the world's port facilities. Major terrorist attacks such as 9/11 have spurred huge investment in port security in recent years and have led to international support for enhancements to the security of transportation and supply chain networks.

The spectrum of security threats that ports face includes not only those associated to terrorism, but also includes traditional foes such as fraud, theft, smuggling, illegal immigration and piracy. Nonetheless the security threat of greatest concern is from terrorist organisations and in particular the delivery of Weapons of Mass Effect (WME) and Weapons of Mass Destruction (WMD), potentially nuclear. As one can imagine ships offer ideal delivery vehicles, not only due to their size and the challenges of accountability of their cargo but perhaps more importantly the reliance on another nation's responsibility to ensure the integrity of its shipping channels. Subsequently the challenge of protecting any nation's ports cannot rely solely on its own counter measures; it must also rely on the security measures in place at the point of origin.

Security challenges

It will be evident for all those interested or involved in ports across the world, that there is a huge amount of activity in the construction of new ports and the expansion of existing ones. Expanding new infrastructure and facilities provides the greatest amount of pressure on the site security management team. During these times of growth they have to deal with two very opposite ends of the spectrum – construction and operations, and this is never easy, especially in a decade where threat levels are on the rise. Extra vigilance is required as the number of construction vehicles increases dramatically and often the site starts to create additional access points like a leaky roof.

The challenges faced by any security plan are now much harder than ever before. Weapons and explosives are easier to obtain and criminal methodologies are often studied in detail with 'lessons learned' articles on the subject openly available. Criminal and terrorist knowledge is spread or promoted via websites, articles and the media, highlighting weakness and vulnerabilities in security plans while introducing concepts and ideas to potential malcontents. Operational planning of a security breach is made easier through information resources and communication tools such as freely available satellite mapping, the target's website, email and mobile phones. Not only this, but the impact of a security related incident can be much greater through an ever hungry, uncensored 24/7 media.

Adaptation

The security industry has had to adapt to these changes, continually changing its form and function to address current and emerging threats. So how has it done this, and how can we continue to improve our resilience against the threats we face. Fortunately, it is not only the threat environment and the capability of potential malcontents that has changed. Security counter measures have also seen remarkable changes in the past few years, through not only advances in technology but with the introduction of new governing regulations and initiatives.

Ports are investing millions annually in the improvement of security measures at their facilities. Security improvements at typical large container ports in 2007 were estimated to cost in the region of US$50 million.

Some of this money is being spent on improving traditional security cost centres such as additional manpower and patrolling, upgrading of perimeter fencing and lighting, improvements in awareness training for security personnel as well as the production of risk and vulnerability assessments, business continuity and crisis management plans, upgrading of security policies and procedure documents, intelligence monitoring and the adoption of governing regulations, which will be discussed later. There is also the costs associated with improving Health and Safety polices and measures. There is currently both conflict and overlap between HSE and Security, where bringing them together would arguably result in greater effectiveness, efficiency and ultimately cost savings. However it is within the technology arena that the lion's share of investment is now being made.

Screening technologies such as RPMs and Gamma/X-Ray imaging devices account for approximately 30 – 50 per cent of investment in today's security planning at ports.

Technology advancement

Technology has advanced considerably over recent times and although some of these large items are very costly, the benefits of providing this additional security for such critical national infrastructure are paramount. Some of the main technologies being incorporated into new and expanding ports are summarised in the following sections:

Screening – screening technologies account for approximately 30 – 50 per cent of investment in today's security planning at ports. Technologies such as Radiation Portal Monitors (RPM) – detection devices that provide passive, non-intrusive screening for radiation emanating from nuclear devices or 'dirty bombs' and large scale Gamma/X-Ray imaging devices allow security personnel to see inside containers in a fast and effective manner. Additionally, security personnel can carry handheld detection devices able to sniff out trace amounts of contraband, explosive and other suspect materials. Some ports are also using similar detection sensors mounted on loading cranes to screen the transfer of containers within the port from one ship to another.

Intelligent surveillance – system manufactures are continually improving the analytical 'brains' of the modern surveillance system. Video analytics and graphical user interfaces (GUI) provide invaluable enhancements to the traditional CCTV monitoring system, reducing the ever increasing pressure on the CCTV operator to dissect a scene for anything suspicious and to help make the decision on the best response. The emergence of network based security systems has allowed system designers to develop modular, future proof and intelligent system designs. Smart systems can also use radar to focus cameras on approaching vessels and automatically track and monitor their movement.

Access control – port authorities need fast, reliable and secure methods to track cargo, vehicles, and personnel moving in, out and around their facilities. Modern access control systems allow just that, with the improvements in biometric technologies as one of the leading examples. Biometrics use unique human characteristics as a form of verification reducing typical weaknesses in badge type systems (such as lost or stolen credentials and misuse). Biometric access control systems are available in a number of forms such as fingerprint, hand and iris recognition and are becoming more widely accepted by security professionals once sceptical over their reliability and accuracy.

Asset tracking – the increasing use of Radio Frequency Identification (RFID) tagging is also improving not only the security of cargo but helping with the logistics and smooth operations of the port. Containers are tagged with unique identification tags that emit radio frequency, providing the capability to track cargo and alert security to any deviation in that cargo's pre-determined path.

ISPS Code

In addition to the advances in technology, recent years have seen the introduction of international standards such as the International Shipping and Port Security (ISPS) Code as well as more controversial mandates such as the US Government's push for the 100 per cent screening of cargo.

On July 1st 2004, the ISPS Code came into effect, introduced by the International Maritime Organisation (IMO). The code is designed to ensure that all parties involved in international shipping (from Port Authorities and ship operators to Contracting Governments) are taking responsibility for the integrity of shipping, 'to deter and detect acts that threaten security'. US borne initiatives such as the Container Security Initiative (CSI), the Customs-Trade Partnership Against Terrorism (C-TPAT) and the Transportation Worker Identification Credential (TWIC) program also work towards enhancing the security of international shipping.

Video analytics and GUI provide invaluable enhancements to the traditional CCTV monitoring system, reducing pressure on the CCTV operator to dissect a scene for anything suspicious and to help make the decision on the best response.

As touched upon above, one of the most significant and contentious additions to the port security industry is the introduction of the US Congress mandate for 100 per cent screening of all US bound containers. Established through the Security and Accountability for Every Port Act (SAFE) of 2006, the 1st July 2012 deadline requires 100 per cent of all US-bound containers to be scanned before entry, affecting the movement of approximately 325 million containers from 600 port container terminals worldwide per year and requiring huge investment in next generation screening equipment.

Security consultants and industry subject matter experts also offer a powerful pool of knowledge that should be exploited by port authorities. International firms, such as U.A.E. based Olive Group, provide clients with industry experts and experienced professionals that can help to build intelligent turnkey security solutions using industry best practice and lesson learned and can advise port authorities on the best use of technology.

Ultimately, the security design for ports should feature an integrated and intelligent security system together with effective procedures, business resilience planning, trained human resources and cooperation with local authorities as well as support from Government level.

These measures and initiatives will of course add to the impact security has on the business end. Not only will port authorities face ever increasing financial commitments, but the productivity at ports will be reduced as security measures, in particular screening, impact the speed of goods and people moving in and around the port. The biggest challenge therefore is perhaps the balance of security with business operations, productivity and ultimately profitability.

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 and South America, Africa and Asia. The company specializes 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.

Olive Group has recently been appointed as the Security Systems Integrator for the Ras Laffan Port Expansion Project, Qatar.

ENQUIRIES

Web: www.olivegroup.com