

PORTS & MARITIME SECURITY AUSTRALIA 2004

Maritime Risk Assessments

Presented by
Paul A. Trebilcock OAM
Executive Director, Intelligent Outcomes Group (IOG)

Introduction

The introduction of new regulatory requirements for designated Australian Maritime Industry Participants (MIP) has provided a number of significant challenges. As the 1 July deadline approaches to have risk assessments complete and security measures implemented to mitigate identified terrorist threats, it is evident that some MIP's, particularly those with a limited understanding of the risk management process, will have difficulty meeting the deadline.

While the ISPS Code provides a standardized, consistent framework for evaluating risk, the lack of specific threat information to enable maritime stakeholders to accurately assess their risks and implement appropriate mitigation strategies is considered a major inhibitor.

The security assessment of Sydney Harbour, which included the international passenger terminals at Sydney Cove and Darling Harbour and multi user facilities at Glebe Island White Bay, was a complex task. The close proximity of national icons and critical infrastructure to the working port introduced a range of threats that have the potential to adversely impact port operations; however, like many other ports in Australia, they are threats that are outside the control of the port authority.

Risk Management Standard

The Australian/New Zealand 4360: 1999 (AS/NZS 4360) Risk Management Standard is the recommended risk management model and is consistent with the IMO ISPS Code requirements. While the AS/NZS 4360 is the accepted standard throughout the Asia-Pacific region and is also used extensively in Europe and North America, there are aspects of the Standard that require further refinement. For example, a number of port operators are having difficulties defining the qualitative measures of likelihood, as defined in AS/NZS 4360.

The measures of likelihood (rare, unlikely, possible, likely and almost certain) need to be tailored to meet the needs of individual MIP's, however, there is no comprehensive explanation of what should be considered during an assessment of the likelihood. Using the current methodology it is also difficult to assess which ports and facilities are at higher risk when compared to others. The determinants for making an informed decision on the likelihood should include an assessment of intent, capability and existing controls.

Threat Identification

Current legislation requires that consultation is to be conducted with relevant national security organisations during the development of maritime risk assessments. In Australia, the Department of Transport and Regional Services (DOTARS) has developed a National Maritime Risk Context Statement to meet this requirement. The Context Statement has been welcomed by the maritime community and provides a useful assessment of the threats currently confronting the maritime industry. However, the inclusion of a more forward looking assessment which identifies which ports and facilities may be at a higher risk than others would be a valuable addition.

The ability for maritime security managers to develop a convincing business case to acquire the necessary funding to enable the implementation of appropriate security measures, commensurate with the assessed level of threat, is a task made more difficult without timely and accurate threat information. While it is acknowledged that DOTARS is seeking to establish trusted networks to enable the timely reporting of changes to the maritime threat environment, the situation highlights the need for State and Territory law enforcement and security agencies to play a more active role.

Port security committees are considered to be fundamental to the successful implementation and maintenance of maritime security assessments and plans. Similarly, the establishment of a Maritime Intelligence Liaison Committee is considered to be equally important, particularly within the major ports, to allow the sharing of more sensitive threat information between the port authority and local law enforcement and security agencies eg. ASIO, Police Counter Terrorist Command, Australian Customs Service and Australian Quarantine and Inspection Service. This initiative would require selected personnel to be security cleared to an appropriate level and key positions eg. Port Security Officer, to be declared a Designated Security Assessment Position.

Additionally, the importance of maritime stakeholder input, at all levels, to inform the risk assessment process cannot be understated.

Gap Analysis

The risk management process should drive any changes to an MIP's security posture. It provides the capacity to evaluate risks and produce a gap analysis of existing security controls.

Intelligent Outcomes Group was responsible for the development of the Critical Infrastructure Risk Manager (CIRM) tool that was used to review critical infrastructure in New South Wales (NSW) following September 11. The CIRM tool was designed specifically to allow the collection and analysis of information relating to the vulnerability of critical infrastructure. The CIRM tool is being used throughout Australia and is now being further developed for use by the State Emergency Management Committee in NSW.

The lessons learnt from the development of the CIRM tool in the critical infrastructure environment have been incorporated into the development of the Intelligent Outcomes all

hazards risk management tool called RiskTrack®. RiskTrack® is compliant with the AS/NZS 4360 standard. The RiskTrack® process is web based and implements an enterprise-wide risk management solution that supports most relational database applications. RiskTrack® provides a proven alternative for MIP's for conducting risk assessments and gap analysis in accordance with the ISPS Code and provides an ongoing capability to monitor changes in threat and related risks.

Next Steps

Despite the 1 July deadline for the implementation of the new ISPS Code requirements, there are a small number of MIP's, particularly in the regional ports, that are only now becoming aware of their regulatory requirements. For these few, given the limited time available, it is recommended that they seek the assistance of a suitably qualified risk management specialist that has the relevant skills and experience in conducting security based maritime risk assessments, as required by DOTARS.

While the primary focus of the implementation process to date has been on preventative measures, maritime stakeholders should also implement reactive measures in the form of business continuity plans. This process will involve the development of strategies to reduce the consequences of a defined terrorist event, should it occur, and ensure that critical port and port facility services and processes can continue.

The implementation of new security measures and plans will require the establishment of a training program for designated security appointments, in accordance with the ISPS Code, and the introduction of security awareness and education sessions for all maritime stakeholders that conduct business within the Security Regulated Port. There will also be an ongoing requirement for MIP's to monitor, review and audit their security risk assessments and plans to ensure that security vulnerabilities are quickly identified and appropriate security measures implemented to mitigate any terrorist threat.