

This document is downloaded from DR-NTU, Nanyang Technological University Library, Singapore.

Title	The maritime security management system : perceptions of the international shipping community
Author(s)	Thai, Vinh Van; Grewal, Devinder
Citation	Thai, V. V. & Grewal, D. (2007). The Maritime Security Management System: Perceptions of the International Shipping Community. <i>Maritime Economics &amp; Logistics</i> , 9, 119–137.
Date	2007
URL	<a href="http://hdl.handle.net/10220/8102">http://hdl.handle.net/10220/8102</a>
Rights	© 2007 Palgrave Macmillan. This is the author created version of a work that has been peer reviewed and accepted for publication by <i>Maritime Economics &amp; Logistics</i> , Palgrave Macmillan. It incorporates referee's comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at: [DOI: <a href="http://dx.doi.org/10.1057/palgrave.mel.9100175">http://dx.doi.org/10.1057/palgrave.mel.9100175</a> ]

# **THE MARITIME SECURITY MANAGEMENT SYSTEM: PERCEPTIONS OF THE INTERNATIONAL SHIPPING COMMUNITY**

**Vinh V. Thai**

Department of Maritime and Logistics Management  
Australian Maritime College  
P.O. Box 986, Launceston, Tasmania 7250, Australia  
Tel.: +61 3 6335 4820 Fax: +61 3 6335 4720  
Email: [V.Thai@amc.edu.au](mailto:V.Thai@amc.edu.au)

*and*

**Devinder Grewal**

Department of Maritime and Logistics Management  
Australian Maritime College  
P.O. Box 986, Launceston, Tasmania 7250, Australia  
Tel.: +61 3 6335 4820 Fax: +61 3 6335 4720  
Email: [D.Grewal@amc.edu.au](mailto:D.Grewal@amc.edu.au)

## **Abstract**

This paper presents the findings of a research project on the Maritime Security Management System (MSMS) conducted at the Australian Maritime College (AMC) in 2005 - 2006. The main objectives of this study are to identify key shore-based and near shore activities associated with maritime operations that are currently not covered by the ISPS Code and players involved in these activities; to explore and analyse important relationships among them which can affect the management of security; to investigate the key criteria of a good/effective security management system; to explore the perceived effectiveness of some major aspects of security activities in a MSMS; and to identify the perceived importance of essential elements in a MSMS. Based on this identification and analysis, essential inputs which should be included in the curriculum of maritime universities and training institutions are proposed. This study applies a two-stage methodological approach, in which a focus group discussion is utilised first to explore the initial ideas from maritime experts, followed by a mail survey to reflect the perceptions of the international shipping community. The findings of this study provide essential insights to the formulation of such a global Maritime Security Management System for the sake of safer and more efficient maritime transport.

*Key words:* Maritime Security Management System, security culture, shore-based activities, security relationships, security elements, security education and training

## **INTRODUCTION**

In recent years, the issue of maritime security has become a major concern on the international maritime agenda. In fact, maritime security dates back to early maritime history under the themes of piracy and cargo theft. The issue has also included stowaways, people and drug trafficking. There have been growing fears that terrorists can also use ships or their

cargo as weapons to attack vulnerable points in the maritime chain just as aircraft were used in the terrorist attack in the United States. Terrorism, thus, becomes the new dimension of maritime security.

There have been a number of responses to this issue. The International Maritime Organisation (IMO) has recently adopted the International Ship and Port Facility Security (ISPS) Code which came into force on July 1<sup>st</sup> 2004, aiming at the establishment of an international framework so that 'ships and port facilities can co-operate to deter and detect acts which threaten security in the maritime transport sector'. Although there has been some research done to address the issues of maritime security from different angles, there are some gaps that need to be taken into consideration. First of all, the coverage of ISPS Code is basically within the traditional interface between ships and port facilities. In addition, only port facilities serving ships engaged in international voyages are covered in the scope of the Code. However, security threats such as cargo theft, stowaways, etc. can exist in all ports serving ships engaged in both domestic and international voyages. Secondly, security threats can come from activities on the shore side. These have not been sufficiently addressed. In the transportation chain, however, maritime security also involves other shore-based activities which can provoke the critical issue of security management connected to maritime transport and operations. For instance, the links with stevedoring companies, road and rail transport companies, freight forwarders, etc. and the relationships among them need to be explored. These are some examples of shore-based activities which are associated with maritime transport and have important implications in the establishment and implementation of a security management system.

A lack of security management system and, on the top of it, a 'security culture', of such shore-based activities will certainly have direct and induced impacts on maritime transport as a whole. A formal research on this aspect is, therefore, considered necessary and useful both from academic and practical perspectives. The following sections describe a research project funded by the International Association of Maritime Universities (IAMU), which aimed to identify all shore-based and near shore activities associated with maritime operations and include them in a global Maritime Security Management System (MSMS), conducted at the Australian Maritime College in 2005-2006.

## **RESEARCH DESIGN AND METHODOLOGY**

There are two main research methods applied in this study. First of all, a focus group discussion through e-mail was utilised to explore ideas and obtain perceptions of experts and operators in the field. Based on this, a postal survey was conducted by sending a questionnaire to the international maritime community. Prospective participants in the focus group were selected from the contact database of the Australian Maritime College. Ten maritime experts in Australia and New Zealand, with their background and expertise being port authorities, harbour masters, marine pilots, port operators, maritime consultants, VTS managers and maritime administrators, were contacted. An e-mail containing the project's background, objectives and methodology was then sent to all participants. Upon confirmation of acceptance, a ten-question questionnaire was sent to all participants. The open-ended questions included in the questionnaire aimed at exploring the experts' perceptions of issues such as whether security initiatives such as the ISPS Code have covered all shore-based and near shore activities, their effectiveness, dimensions of security activities to be included in the MSMS, relationships in the system, criteria for a good/effective system as well as what should be incorporated in the contemporary curriculum of maritime universities and other training

institutions in order to address the full aspects of maritime security. Other inputs which they felt were necessary for the MSMS were also invited.

The responses of the participants were subsequently collated with author-related links removed, then synthesised and analysed into a single document. This was then sent around to all participants for their comments and additional inputs before being finalised. Upon completion of this process, the final version of the discussion analysis was devised. Based on this analysis, a detailed postal questionnaire was developed and sent around to participants again as a pilot study for their comments. It was then verified and finalised for being sent out to the international shipping community, together with a cover letter explaining the background and objectives of the study. The postal questionnaire contained seven questions addressing issues identified through the analysis of the focus group discussion, and four general questions asking about demographic information of the respondents. Since the topic of this study is exploratory in nature, the questions designed were purposely of both close- and open-ended types so as to provide respondents with an opportunity to expand upon or explain their answers. Space was also provided on the questionnaire for additional written comments, with the purpose of encouraging the respondents to contribute as much additional details for their answers as possible. Most questions were measured using Likert and numerical scales, since the main purpose of the questionnaire was to explore the attitude of respondents towards related issues being surveyed. Measurement was constructed on five-point scale, ranging from 1 (strongly agree, most effective, very important) to 5 (strongly disagree, least effective, not at all important).

The design of the postal survey was decided through the analysis of the focus group discussion. Potential respondents targeted for the survey included port authorities/harbour

masters, port operators/stevedoring companies and shipping companies. The sampling frame for this survey was thus chosen from World Shipping Directory of Fairplay (Fairplay World Shipping Directory, 2006). Using the simple random probability sampling method, a mailing list containing 298 target respondents, of which 67 were port authorities, 112 were shipping or ship management companies, and 126 were port operators/stevedoring companies was finalised for the postal survey. In an effort to increase the response rate of the postal survey, the questionnaire was also posted on the website of the AMC. By the cut-off date, there were 60 returned answers to the questionnaire received via both mail and electronic means (on-line questionnaire). This represented a 20% response rate.

## **PERCEPTIONS OF THE MSMS**

The main findings in this research, synthesized both from the focus group interviews and survey, are provided below.

### **The need to extend current security initiatives**

The ISPS Code aims at enhancing maritime security on board ships and at the ship/port interface by providing a standardised and consistent framework for the evaluation of risks. As mentioned earlier, the main focus of the ISPS Code is on the sea leg where the ships are at sea and face many security threats, as well as the interface between ships and port facilities when ships are at berths. The coverage of the Code does not reach the shore-based and near shore areas whereas many activities can provoke security threats to the whole maritime transport chain.

This can also be seen clearly in the issue of container security, due to the importance of containerisation for international trade. At the same time, there has also been a paradigm shift

of focus regarding perceptions on security of containers. Before the threat of terrorism in maritime transport was recognised, the traditional approach to container security was in keeping the goods that were supposed to be in the box, in the box. Given the renewed terrorist threats, especially the scenario that terrorists can use containers to conceal and deliver weapons of mass destruction (WMD), there is added responsibility to ensure that things that are not supposed to be in the box are actually kept out of the box (Eyefortransport, 2002). To ensure the integrity of containers has thus become a critical matter of security, since the integrity of container will affect the security of cargo inside containers, and therefore, the security of maritime transport services (RAND, 2003). However, characteristics of the container transport system also create some difficulties for security efforts. For example, the movement of each container is part of a transaction that can involve up to 25 different parties: buyers, sellers, inland freighters and shipping lines, middlemen (customs and cargo brokers), financiers and governments. A single trade can generate 30-40 documents, and each container can carry cargo for several customers, thus multiplying the number of documents further (Economist, 2002). Such a complexity of the container transport system triggers the need to address the security of this system within a comprehensive intermodal framework integrating measures across the entire container transport chain. While such a framework may exist covering ports and maritime transport, there is not yet an analogous framework for inland transport (RAND, 2003; OECD, 2004). This implies the fact that while there has not been any such a framework, it is critical to promote a self-regulation culture involving security as similar as what the ISM Code is aiming for safety in maritime transport.

There is a high level of consensus among members of the focus group regarding this issue as they agreed that the ISPS Code should be extended to cover other shore-based and near shore activities in the whole transport chain. There are several justifications for this. The most

prevailing reason behind the consensus is that the contemporary security paradigm does not seamlessly interface all other modes of transport, since they focus mainly on the ship–shore interface point. This is aligned with the current literature on maritime security. Specifically, it is argued that many security threats can actually materialise ashore in the hinterland of ports and with other land transport modes rather than shipping. Furthermore, most of the focus group members felt that there are still some omissions that prevent the current security initiatives from being effective in implementing effective security management ashore. In this connection, most focus group members argued that the current initiatives rely on the ‘detect and deter’ philosophy. Therefore, the capability to respond to security incidents relies on arrangements on counter terrorism response which are beyond the ISPS code. Besides, the effectiveness of the ISPS Code depends on the integrity of the various security plans and the arrangements made by the custodians of these plans. The effectiveness of the security management system depends very much on the continuous review and update of security plans. It is with this in mind that, when assessing the capability and effectiveness of the current security initiatives, some members argued that they are only effective if the point of origin of an export shipment is based within the port precinct, otherwise there is no supply chain security mentality.

Clearly, from the above, the perception is that current security initiatives need to extend their coverage, including other shore-based and near shore activities which can lead to security breaches. It is also affirmed that, when researching the issue of maritime security management system, one needs to take a holistic approach considering maritime security in the broader spectrum of total transport security or supply chain security including all modes of transport and the interfaces between them.

### **The issue of security in maritime organisations**

To begin the survey of the international shipping community's perceptions of pertinent issues in a MSMS, respondents were asked to indicate their general view on the issue of maritime security in their organisations. The purpose of this question was to explore respondents' general perceptions of this issue after a period that maritime security was given much focus. Answers to this question also indicate the magnitude of the research problem in this study and stress the importance of issues being investigated. Respondents expressed a high consensus toward the issue of maritime security, in which 70% viewed it very important and a top priority, while the remaining 30% perceived it as a quite important issue in their organisations. It is evident that maritime security is a very important issue in shipping organisations, and thus a thorough investigation of related aspects in a maritime security management system would prove to be worthwhile.

### **Activities to be included in a holistic MSMS**

In formulating any operation and management system, the identification of related activities in such a system is probably the very first task to be completed. In this survey, the activities which should be included in a holistic MSMS were identified through literature review, as well as synthesised from the focus group discussions. Results of descriptive statistical analysis are presented in Table 1 below.

*Insert Table 1 about here*

It can be seen from Table 1 that all activities which should be included in a MSMS as identified in the literature and focus group discussion are confirmed by survey respondents with all mean answers smaller than 3, which is the neutral point of the scale. In this list, *stevedoring*, consisting of cargo handling activities in all operation systems within port and terminal area, receives the highest consensus from respondents, while the activity which has

the lowest mean score in the list is *cargo operations in the port's hinterland*. Yet, it is still evident, based on mean response to this activity, that it is closely related with maritime security and as a matter of fact it can seriously compromise it. The above results show that activities to be incorporated in a MSMS should be viewed through a holistic perspective. These activities encompass not only ship operations at sea, but also the navigation of ships in channels, cargo operations in port and terminal areas and are extended to the points where cargoes are transferred from one to another mode of transportation and operations of cargo at nodes in the port hinterland. In other words, the MSMS should cover all activities in the maritime transportation chain, or from the point where cargoes are placed in the custody of a transport operator until they are delivered to the consignee.

Many respondents proposed some additional activities to be included in the maritime security management system, such as access of visitors, passengers and crew to port and terminal areas, ship operations in coastal waters of civil war countries, ships operations in anchorage, and ship operations in dry-docks or repair yards. While these additional activities are also associated with maritime security problems, ship operations in coastal waters of civil war countries could be included in the ship operations at sea activities, whereas ship operations in anchorage would actually be covered in the scope of ship operations while in channel. The other two activities, i.e. access of visitors, passengers and crew to port and terminal areas; and ship operations in dry-docks or repair yards, are valid and can be taken into the list as new activities to be included in a holistic MSMS. This is because many governments do not consider dry-docks and repair yards as ports or port facilities to be covered in the ISPS Code, and the management of access to port areas of passengers, visitors and crew is important to assure security as well.

### **Players involved in a holistic MSMS**

The next important task is to explore the key players in such a system. Again, through literature review and analysis of the results of focus group discussions, a list of players who should be involved in a holistic MSMS is proposed to the international shipping community. Table 4 presents a summary of descriptive statistical analysis of respondents' perceptions of the proposed players in the system. There is a high consensus between survey respondents and focus group members toward the proposed players in the MSMS. The survey indicates that all transport operators involved in the cargo operation chain, e.g. land, sea, and air transport operators, should be the key players in the management of maritime security. Survey respondents agreed the least on cargo owners as involved players in such a security management system; however the mean response to them indicated that these players have an important role in the management of maritime security. This is valid since cargo owners are the very first players who deal directly with cargo security in the whole maritime logistics chain, and thus their positive attitude toward the issue is critical to make security management effective. This is also the key argument in the U.S. C-TPAT (Customs-Trade Partnership Against Terrorism) program.

*Insert Table 2 about here*

While all proposed players to be involved in a holistic MSMS were accepted by survey respondents, they also indicated some other additional players to be included in such a system. For example, some respondents argued that law enforcement agencies such as customs, health and sanitary services, and other maritime industry participants (MIPs), also play an important role in dealing with maritime security effectively. Other respondents suggested that shipping- and port agents should also be included in the system, as their awareness of the maritime security issue has a great implication on whether the management of maritime security could be effectively conducted. Indeed, the maritime security chain is only as strong as each link in

the chain, thus irresponsible behaviour of a single player could jeopardise the effectiveness of the whole system. Therefore, shipping and port agents are also included in the MSMS as key players involved.

### **Importance of major organisational relationships**

The relationships among players in any management system are critical since the effectiveness of the system is closely associated with the strength of these relationships and whether the players in the system cooperate and interact with each other to smoothly solve any arising problem. In fact, virtually all relationships among players, directly and indirectly involved in the MSMS, are important; however, survey respondents emphasised their perceptions of the importance of a number of organisational relationships between key players as in Table 3. These relationships encompass the organisational connections both between the transport operators and their external stakeholders, as well as between the management and operational staff levels within each organisation involved in the MSMS. It is evident from Table 3 that the relationship between each transport operator and their security service providers is perceived as the most important in the MSMS; the least important, as perceived by survey respondents, was the relationship between each transport operator and their stakeholders. Nevertheless, the mean score of responses to this relationship was 1.72, implying that the cooperation and coordination between each transport operator and their direct and indirect customers also play a critical role in the effective management of security problems in maritime logistics operations.

*Insert Table 3 about here*

### **Effectiveness of key security aspects**

Security aspects refer to various groups of activities in a security management system such as the education and training for enhanced security awareness, access control meaning the control of physical access to infrastructures, i.e. ships at berth, yards and warehouses, or procedural security which refers to security procedures to protect against un-manifested material being introduced into the cargo flow in maritime transport, such as the verification of seals on containers. An MSMS would include many aspects of the security management practice such as procedural security, access control, etc., and the focal point is that the effectiveness of each aspect should be evaluated. This is essential, since it helps to set the prioritised security areas which governments and organisations should concentrate on and allocate their scarce resources effectively. Since maritime security is just another type of risk governments and organisations involved in the maritime logistics operations are facing everyday, the assessment and mitigation of security threats should closely follow the standards of risk management practices, in which all possible risks should be clearly identified and prioritised. Indeed, the identification of security aspects/dimensions and their effectiveness can play an important role in the management of maritime security.

Literature review and analysis of focus group discussion conducted earlier suggest that there are a number of security aspects which governments and organisations in the MSMS should focus upon. Results of descriptive statistical analysis are presented in Tables 4 below.

*Insert Table 4 about here*

It is evident from Table 4 that education and training in security awareness is the most effective aspect in managing security in maritime logistics operations. Information security, for instance, the safety and integrity of the system issuing bill of lading, cargo manifest and other related commercial data in a shipping company, is seen as the least effective security aspect. However, its mean score from Table 4 implies that the management of this security

aspect would be important as part of governments' and organisations' strategies leading to good security management results. Results from this table also confirm that, while the role of 'technical aspect' in security management is increasingly important, the human factor is still the decisive element for the success of the maritime security management system. Indeed, as people are the centre of any operations and management system, the education and training of human awareness play the critical role. As human awareness is enhanced, all other security aspects in the system such as access control, physical or procedural security can be appropriately and effectively managed, and the synergy of all these aspects/dimensions would contribute to the success of the system as a whole.

### **Importance of essential security elements**

Security elements are related to various components in a security management system such as technology, people, process, policy, etc. Many organisations view security in a narrow sense as a technology-driven issue, and that technology can solve all security problems in the organisation. In fact, it has been argued that technology alone cannot eliminate all exposures to security threats and there are other essential elements that have to be taken into consideration if the management of security is to be effective. In this connection, Hamilton (2004) argues that effective security can never be achieved by relying on technology alone, as people will always play a fundamental role in all phases: from planning to implementation and to enforcement. Accordingly, technology and people must work together as part of an overall security process, beginning with a risk management approach. Wiederin *et al.* (2002) emphasise that processes, policies, procedures and people, along with best-of-breed security technology (products), constitute a complete security offering. These elements relate to each other as follows:

- (1) People follow processes and procedures laid out in policies;
- (2) People are educated in the processes, procedures and policies;
- (3) Processes define life cycle activities that are customised in policies and procedures;
- (4) Processes can include technologies;
- (5) Procedures are the detailed steps involved in applying processes and technologies;
- (6) Policies describe how people are expected to comply with the processes and procedures.

Such a comprehensive and interrelated approach is needed for the effective management of security in the organisation. Providing effective security requires a comprehensive approach that considers a variety of areas both within and outside of the area in question. The C-TPAT initiative of U.S. Customs, for instance, considers supply chain security in six elements, namely, *procedural security*, *physical security*, *access controls*, *personnel security*, *education and training awareness*, and *conveyance security*. Healy (1968) argues that the need for interdependence and interrelation of security functions in the organisation is not limited to physical controls, but must be applied to the entire security program. It should be emphasised that physical controls are only one technique of providing security and these controls by themselves cannot be relied on to give complete protection. The lack of complete security plan can have the effect described in the well-known maxim attributed to George Herbert in the 17<sup>th</sup> century: “for want of a nail the shoe is lost, for want of a shoe the horse is lost, for want of a horse the rider is lost”. Benjamin Franklin’s comment in 1757 might also be applied: “a little neglect may breed mischief” (cited in Healy 1968). The effective management of security in the organisation should therefore be designed to provide complete security coverage, including a variety of security functions such as physical security, personnel security, security of documents, emergency and disaster, etc. A holistic,

comprehensive and integrated approach is therefore considered essential to the success of security management in the organisation.

The maritime security management system is a network of various elements which have reciprocal relationships with each other. The review of relevant literature and analysis of focus group discussions conducted in the early stages of this study revealed that several essential elements, such as such as policy, people, process, communication, etc. and a number of their combinations, would be very important for the purpose of effective management of security in maritime logistics operations. Table 5 provides the summaries of descriptive statistical analyses of these elements' perceived importance. It is noted that all elements of the security system identified in the literature and focus group discussions were confirmed by the survey respondents.

*Insert Table 5 about here*

It is evident from Table 5 that *people* are the most important element in the maritime security management system. The combination of *processes* and *systems/technology* is ranked the least important element in the MSMS, however the high mean score of this element also emphasises its importance for the successful management of MSMS and implies that there is a high consensus among survey respondents. It is interesting to note that the human factor is placed at the centre and is the focus of MSMS. It is consistent throughout the survey results that the human factor is always seen as the most important dimension and element in the security management system. Earlier, it is revealed that *security awareness education and training* is seen as the most effective security aspect/dimension, meaning that security control and management must start from the education of security awareness for the people who are directly and indirectly involved in the maritime logistics operations. Concurrently, the importance of *people* and a number of combinations of this element, such as *people and*

*communication, people and processes, people and systems/technology* are highly perceived. It is thus evident that maritime security is, by nature, about people and it should begin with the people. The effectiveness of the maritime security management system is thus very much related to how people view security in their organisations, and whether sufficient education and training are provided to people so that they can effectively identify, analyse, assess and treat maritime security risks.

### **Key criteria of a good/effective MSMS**

Literature and focus groups discussions conducted in the early phase of this study have revealed a number of criteria to be considered when assessing whether a maritime security management system is good or effective. They were also incorporated into the postal questionnaire for the purpose of surveying the international shipping community. Table 6 summarises the descriptive statistical analysis of responses to the proposed 15 criteria of a good/effective MSMS, showing that all proposed criteria are valid and should be considered as essential for assessing the effectiveness of a MSMS.

*Insert Table 6 about here*

Respondents agreed that an effective MSMS should have *effective communication among the participants of the security system*. The importance of *good security information and intelligence* was also highlighted, while respondents least agreed that *designated and adequately equipped emergency control centres* are a criterion of a good/effective MSMS. However, the high mean score of this criterion also implies that it should be retained in the list of criteria for assessing a good/effective maritime security management system.

### **Essential inputs in the curriculum of security education and training**

Having identified all essential components, together with the criteria of a good/effective MSMS, it is critical that governments and organisations involved in security management in maritime logistics operations clearly see the requirements imposed on such a system. In order to have sufficient and adequate resources in effectively managing maritime security risks, education and training plays an important role. This provokes the question of how maritime universities and other training institutions design their curriculum to respond adequately to the demand from the industry regarding maritime security management. Literature review and analysis of focus group discussions showed that there are various inputs to be incorporated in the contemporary curriculum of maritime universities and other training institutions in this respect. It is now important to explore whether there is consensus among the international maritime community. Survey respondents in this study were asked to indicate their perceptions of the proposed inputs in the contemporary curriculum of maritime universities and other training institutions so as to meet the demand from the industry practices. Table 7 below indicates the summary of descriptive analysis of responses.

*Insert Table 7 about here*

It is evident from Table 7 that all proposed curriculum inputs are accepted by respondents as essential for the development of relevant courses addressing maritime security issues. Furthermore, there is the highest level of consensus among survey respondents toward the curriculum input of *holistic risk management principle applied to international supply chain and intermodal transport*. The least agreed curriculum input is *transport security in a broader perspective of international supply chain and intermodal transport*. Nevertheless, this curriculum input should be retained on the proposed list, since its mean score is sufficient to justify its presence in the curriculum.

The scope of components to be included in a global Maritime Security Management System, together with criteria of a good/effective MSMS and necessary curriculum inputs for education and training are summarised in Figure 1 below.

## **CONCLUSION**

In this paper, we present the findings of a study investigating basic elements of a global Maritime Security Management System. These elements have been identified, analysed and discussed, taking into consideration the need to extend the ISPS Code which is currently applied only for the ship operations at sea and ship/port interface. The results of this study reveal that there is a high level of agreement between members of the focus group and respondents from the international shipping community with regards to key issues raised in this study, indicating that its findings are reliable and helpful for the subsequent formulation of such a Maritime Security Management System for the sake of safer and more efficient maritime transport.

## **BIBLIOGRAPHY**

Fairplay World Shipping Directory (2006). <http://www.wsdonline.com/>, accessed 15 August 2004.

Eyefortransport (2002). Cargo security overview: technologies, government and customs initiatives, <http://www.eyefortransport.com/index.asp?news=33800&ch=159>, accessed 15 April 2004.

RAND (2003). Seacurity: improving the security of the global sea-container shipping system, <http://www.rand.org/publications/MR/MR1695/MR1695.pdf>, accessed 15 September 2003.

Economist (2002). When trade and security clash, *The Economist*, 4 April, [http://www.economist.com/business/displayStory.cfm?story\\_id=1066906](http://www.economist.com/business/displayStory.cfm?story_id=1066906), accessed 5 May 2004.

OECD (2004). Report on container transport security across modes, <http://www.oecd.org/dataoecd/29/8/31839546.pdf>, accessed 15 July 2004.

Hamilton, CR (2004). The case for holistic security: the integration of information and physical security as an element of homeland security, [http://www.riskwatch.com/Press/Holistic\\_Security\\_10-03.pdf](http://www.riskwatch.com/Press/Holistic_Security_10-03.pdf), accessed 15 May 2004.

Wiederin, S., Wurster, D., Hoefelmeyer, RS and Phillips, T (2002). The true meaning of security, <http://www.rrtidd.com/webQuests/shared/true%20Meaning%20of%20Security.pdf> , accessed 30 July 2003.

Healy, RJ (1968), *Design for security*, John Wiley & Sons: New York.

## Figures and Tables

Table 1: Attitude towards activities in a MSMS

Activities	Mean	STD
Stevedoring (cargo handling in all operation systems within port and terminal area)	1.30	0.56
Ship operations at sea	1.42	0.65
Ship operations while in channel	1.42	0.70
Ship berthing/unberthing	1.43	0.62
Cargo operations at transport interfaces	1.62	0.56
Cargo operations in the port's hinterland	1.70	0.53

Note: 1 = strongly agree, 5 = strongly disagree.

Table 2: Attitude toward players in a MSMS

Players	Mean	STD
Transport operators	1.20	0.40
Government authorities	1.28	0.49
Port authorities	1.33	0.48
Security service providers	1.48	0.77
Cargo owners	1.53	0.54

Note: 1 = strongly agree, 5 = strongly disagree.

Table 3: Importance of relationships in a MSMS

Relationships	Mean	STD	Rank
Between each transport operator and their security service providers	1.47	0.50	1
Between the government (regulator) and transport operators	1.50	0.50	2
Between players in the MSMS	1.58	0.59	3
Between management and staff within the organisation regarding security accountability and responsibility	1.62	0.58	4
Between each transport operator and their stakeholders	1.72	0.64	5

Note: relative ranking based on mean scores; 1 = very important, 5 = not at all important.

Table 4: Perceived effectiveness of security dimensions in a MSMS

Dimensions	Mean	STD	Rank
Security awareness education and training	1.23	0.53	1
Access control	1.28	0.49	2
Physical security	1.57	0.59	3
Procedural security	1.58	0.62	4
Personnel security	1.67	0.48	5
Information security	1.88	0.45	6

Note: relative ranking based on mean scores; 1 = most effective, 5 = least effective.

Table 5: Importance of security elements in a MSMS

Elements	Mean	STD	Rank
People	1.18	0.39	1
Communication	1.20	0.40	2
Policy	1.30	0.46	3
People and communication	1.40	0.49	4
People and processes	1.43	0.50	5
Processes/procedures	1.45	0.50	6
Systems/technology	1.67	0.54	7
Communication and technology	1.72	0.45	8
People and systems/technology	1.77	0.43	9
Processes and systems/technology	1.85	0.52	10

Note: relative ranking based on mean scores; 1 = very important, 5 = not at all important.

Table 6: Attitude towards criteria of a good/effective MSMS

Criteria	Mean	STD
Effective communication among the participants of the security system	1.17	0.38
Good security information and intelligence	1.23	0.53
To be holistic in the consideration of the risk assessment at appropriate intervals	1.27	0.45
Constant reviewing of security processes, procedures and available technology	1.40	0.49
Security should become part of the wider safety management system	1.42	0.62
Meaningful government inputs in terms of resources support and legislative guidance	1.48	0.50
Adequate funding and government guidelines	1.58	0.72
Frequently conducting security drills and exercises	1.58	0.53
Legislative background and policy formation	1.62	0.61
Developed and effective relationships within the organisation and between organisations in the security management system	1.65	0.55
Consistency in application of systems, processes and protocols – to the extent that it is possible, as in other regulatory matters, in the global context	1.67	0.66
Security management should be integrated within the spectrum of risk management, quality management, environmental management and other safety systems	1.72	0.52
Auditable metrics, monitoring and reporting procedures in place	1.73	0.45
Regular security training	1.75	0.79
Designated and adequately equipped emergency control centres	1.78	0.45

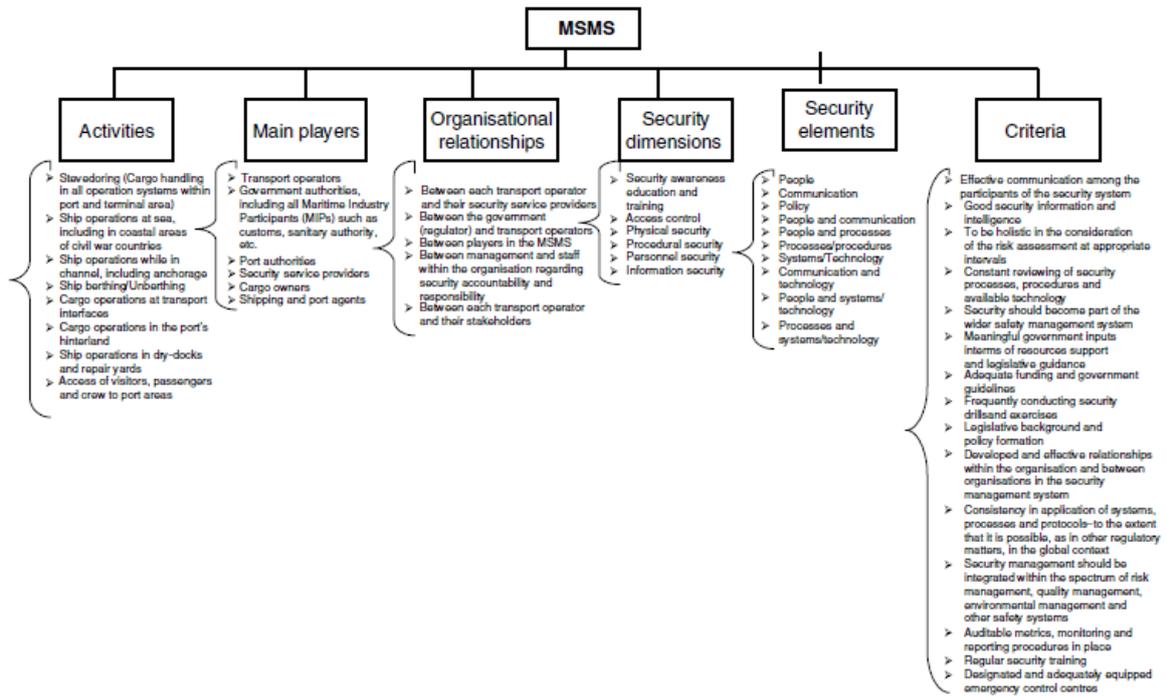
Note: 1 = strongly agree, 5 = strongly disagree.

Table 7: Attitude towards inputs of curriculum for education and training needs

Inputs	Mean	STD
Holistic risk management principle applied to international supply chain and intermodal transport	1.65	0.58
An approved course based on guidelines from IMO involving all aspects of a Maritime Security System	1.73	0.61
Security in current maritime and logistics management course, including port and terminal management	1.80	0.80
International and national issues relating to security management in international supply chain and maritime transport, including security initiatives and strategies to effectively implement them	2.05	0.79
Transport security in a broader perspective of international supply chain and intermodal transport	2.20	0.82

Note: 1 = strongly agree, 5 = strongly disagree.

Figure 1: Features of an MSMS.



## APPENDIX: THE POSTAL QUESTIONNAIRE

### STUDY ON MARITIME SECURITY MANAGEMENT SYSTEM (MSMS)

1. How do you see the issue of maritime security in your organisation?

*Very important/Top priority*                       *Quite important*                       *Other*

2. Please indicate your view on the following statements, where **1** = ‘strongly agree’, **2** = ‘agree’, **3** = ‘neutral’, **4** = ‘disagree’ and **5** = ‘strongly disagree’.

2.1 A holistic MSMS should include the following activities:

(a) Ship operations at sea	1	2	3	4	5
(b) Ship operations while in channel	1	2	3	4	5
(c) Stevedoring (Cargo handling in all operation systems within port and terminal area)	1	2	3	4	5
(d) Ship berthing/Unberthing	1	2	3	4	5
(e) Cargo operations in the port’s hinterland	1	2	3	4	5
(f) Cargo operations at transport interfaces	1	2	3	4	5
(m) <i>Others (please specify)</i>					
	1	2	3	4	5
	1	2	3	4	5
	1	2	3	4	5

2.2 A holistic MSMS should involve the following players:

(a) Transport operators (Shipping lines, port operators, freight forwarders, land transport operators, etc)	1	2	3	4	5
(b) Cargo owners	1	2	3	4	5
(c) Security service providers	1	2	3	4	5
(d) Port authorities	1	2	3	4	5
(e) Government authorities	1	2	3	4	5
(m) <i>Others (please specify)</i>					
	1	2	3	4	5
	1	2	3	4	5
	1	2	3	4	5

2.3 A good/effective MSMS should possess the following key criteria:

(a) To be holistic in the consideration of the risk assessment at appropriate intervals	1	2	3	4	5
(b) Designated and adequately equipped emergency control centres	1	2	3	4	5
(c) Effective communication among the participants of the security system	1	2	3	4	5
(d) Constant reviewing of security processes, procedures and available technology	1	2	3	4	5
(e) Frequently conducting security drills and exercises	1	2	3	4	5
(f) Developed and effective relationships within the organisation and between organisations in the security management system	1	2	3	4	5

(g) Legislative background and policy formation	1	2	3	4	5
(h) Auditable metrics, monitoring and reporting procedures in place	1	2	3	4	5
(i) Adequate funding and government guidelines	1	2	3	4	5
(j) Good security information and intelligence	1	2	3	4	5
(k) Regular security training	1	2	3	4	5
(l) Meaningful government inputs in terms of resources support and legislative guidance	1	2	3	4	5
(m) Consistency in application of systems, processes and protocols – to the extent that it is possible, as in other regulatory matters, in the global context	1	2	3	4	5
(n) Security should become part of the wider safety management system	1	2	3	4	5
(o) Security management should be integrated within the spectrum of risk management, quality management, environmental management and other safety systems	1	2	3	4	5
(j) <i>Others (please specify)</i>					
	1	2	3	4	5
	1	2	3	4	5
	1	2	3	4	5

2.4 The followings are essential inputs which should be included in the current curriculum of maritime universities and other training institutions so as to provide education and training of vital components of a good/effective MSMS:

(a) An approved course based on guidelines from IMO involving all aspects of a Maritime Security System	1	2	3	4	5
(b) Holistic risk management principle applied to international supply chain and intermodal transport	1	2	3	4	5
(c) Security in current maritime and logistics management course, including port and terminal management	1	2	3	4	5
(d) Transport security in a broader perspective of international supply chain and intermodal transport	1	2	3	4	5
(e) International and national issues relating to security management in international supply chain and maritime transport, including security initiatives and strategies to effectively implement them	1	2	3	4	5
(j) <i>Others (please specify)</i>					
	1	2	3	4	5
	1	2	3	4	5
	1	2	3	4	5

3. In your opinion, please indicate the effectiveness of the following aspects in the security activities you identified above in a MSMS, where **1 = ‘most effective’, 2 = ‘effective’, 3 = ‘neutral’, 4 = ‘not very effective’ and 5 = ‘least effective’.**

(a) Procedural security	1	2	3	4	5
(b) Physical security	1	2	3	4	5
(c) Access control	1	2	3	4	5
(d) Personnel security	1	2	3	4	5
(e) Information security	1	2	3	4	5
(f) Security awareness education and training	1	2	3	4	5

(m) <i>Others (please specify)</i>					
	1	2	3	4	5
	1	2	3	4	5
	1	2	3	4	5

4. Please indicate the importance of the following relationships in a MSMS, where **1 = 'Very important', 2 = 'important', 3 = 'neutral', 4 = 'not important' and 5 = 'not at all important'**.

(a) Between management and staff within the organisation regarding security accountability and responsibility	1	2	3	4	5
(b) Between the government (regulator) and transport operators	1	2	3	4	5
(c) Between each transport operator and their stakeholders	1	2	3	4	5
(d) Between each transport operator and their security service providers	1	2	3	4	5
(e) Between players in the MSMS	1	2	3	4	5
(i) <i>Others (please specify)</i>					
	1	2	3	4	5
	1	2	3	4	5
	1	2	3	4	5

5. Please indicate the importance of the following elements, or the combination of elements, in a MSMS, where **1 = 'Very important', 2 = 'important', 3 = 'neutral', 4 = 'not important' and 5 = 'not at all important'**?

(a) Policy	1	2	3	4	5
(b) People	1	2	3	4	5
(c) Processes/procedures	1	2	3	4	5
(d) Communication	1	2	3	4	5
(e) Systems/Technology	1	2	3	4	5
(f) People and processes	1	2	3	4	5
(g) People and systems/technology	1	2	3	4	5
(h) People and communication	1	2	3	4	5
(i) Processes and systems/technology	1	2	3	4	5
(j) Communication and technology	1	2	3	4	5
(i) <i>Others (please specify)</i>					
	1	2	3	4	5
	1	2	3	4	5
	1	2	3	4	5

6. In order to achieve successful implementation of the MSMS do you perceive any other issues or factors to be considered? *(Please attach a separate page if more space is needed)*

.....

.....

7. Do you have any other comments on this study? *(Please attach a separate page if more space is needed)*

.....

.....

8. Your name: ..... Designation: .....

9. Organisation: .....

10. You are a:

*Port authority/Harbour Master*       *Shipping company*   
*Port operator/Stevedoring company*       *Other (Please specify)*

11. Would you like to receive a copy of this report?

*Yes*       *No*

*Address for correspondence (Email is preferable):* .....

**Thank you very much for your valuable contribution to this study.**