Effective maritime security : conceptual model and empirical evidence

Thai, Vinh Van

2009

Thai, V. V. (2009). Effective maritime security: conceptual model and empirical evidence. Maritime Policy & Management, 36(2), 147-163.

https://hdl.handle.net/10356/98496

https://doi.org/10.1080/03088830902868115

EFFECTIVE MARITIME SECURITY: CONCEPTUAL MODEL AND EMPIRICAL EVIDENCE

Vinh V Thai
Department of Maritime and Logistics Management
Australian Maritime College
Locked Bag 1397, Launceston, Tasmania 7250, Australia
Tel.: +61 3 6335 4764 Fax: +61 3 6335 4720
Email: vvthai@amc.edu.au

Abstract

In recent years, the issue of maritime security has become a major concern on the international maritime agenda. One of the issues in this respect is how to enhance security while not jeopardising organisational efficiency and effectiveness, or to manage security effectively, e.g. facilitating the smooth flows of materials while enhancing supply chain security at the same time. In addressing this issue, we place three cornerstones for the effective management of security in maritime transport: quality management (QM), risk management (RM), and business continuity management (BCM). A conceptual model of effective maritime security, including 13 dimensions and 24 associated critical success factors, is devised following this reasoning. The model was tested through a survey of 119 maritime transport organisations and 25 interviews conducted in Vietnam. Findings support that all proposed 24 factors are valid and should be used as critical factors for success in effectively managing security in maritime transport, in that those involving security incident handling and response are rated as the most important in magnitude, along with security risk assessment, risk-based security mitigation strategies and plans, and senior management commitment and leadership. Managers can use the model designed and tested in this research to develop a checklist of essential components for their company's security management policies, strategies, and plans. The use of a universal checklist to evaluate maritime security management would also greatly facilitate benchmarking across organisations in the industry.

***Keywords**: effective maritime security, critical success factor, quality management, risk management, business continuity management, security management*

1. Introduction

In recent years, the issue of maritime security has become a major concern in the international maritime agenda. Maritime security dates back to early maritime history under the themes of piracy and cargo theft and now includes also stowaways, people and drug trafficking, information security and, of course, maritime terrorism after the September 11th event. The objective of security management is to support the organisations in achieving their business goals and objectives. From the management point of view, security threats in maritime transport should be viewed as one of the risks in the organisation's risk profile. The management of security in maritime transport is therefore a management and business issue rather than the compliance with international security conventions. However, there have been some arguments that heightened security measures would hamper the international trade and have negative impacts on business results. With this background, one of the fundamental questions is how to achieve effective maritime security, e.g. satisfying security requirements while enhancing other business objectives, such as service quality or operational efficiency. In other words, it is important to identify and comprehend the critical success factors (CSFs) for the effective management of security in maritime transport.

In this paper, we aim to seek the answer for that question. While there have been some studies insisting risk-based solutions for security problems, there has been little research about effective maritime security from the holistic perspective. Since security is repeatedly found to be an element of service quality especially in maritime transport, it could be argued that the quality management approach to security management would also be useful to obtain effective security outcomes. The main purpose of this empirical research is thus to contribute to the theory building, as well as management practice of effective security. In particular, the major objectives of this research are to identify critical factors of effective maritime security and empirically validate them. The remainder of this paper is organised as follows.

First, conceptual foundation is presented in that various approaches to effective maritime security are analysed and discussed. Based on this, the critical success factors (CSFs) of effective maritime security are identified. Empirical validation of these CFSs is presented next with research methodology described and findings discussed. The paper concludes with recommendations for future extension of this research.

2. Conceptual foundation: The Quality Management (QM) approach to effective maritime security

2.1 Security prevention from the source

Good security does not mean inspection, but rather security prevention from the source. In supply chain and maritime transport, if security is equivalent to final inspection, it has to be relied on inspection of cargo shipments down the chain at the ports of destination or at border crossings [1]. Heightened security inspections in this respect are highly costly, and more importantly, they can potentially lead to congestion and delays added up in the chain. For instance, in response to security threats, if governments call for an increased inspection rate of cargoes, containers and transportation vehicles, this will lead to the pile-up of containers at ports around the globe. Clearly, similar to quality management, such a reliance on final inspection to ensure security will not provide organisations with expected results, and therefore the prevention from the source philosophy should be applied instead. In manufacturing sector, the way to eliminate inspections is to design and build in quality from the start. The analogy in supply chain and maritime transport security is to design and apply processes that prevent tampering with a shipment before, during, and after the loading process [1], [2]. Prevention from the source in supply chain and maritime transport security management implies that all necessary processes to ensure security need to be designed and built in right from the beginning of the shipment movement along the chain, so as to make everything right the first time.

2.2 Process control and management for security purpose

In quality management, in-process quality control and management is needed to ensure that variability during the process is driven out. Similarly, the prevention from the source in security management must be followed by in-process control in order to monitor shipments while they are in transit and thus significantly reduce the risks of shipment being tampered. Operating processes of shipment movements must be designed and built in so as any tampering of the shipments have to be detected, and mitigation measures to be immediately deployed at due time. Like quality, security should be built in from a project inception.

2.3 Total organisational focus in security management

In quality management, total organisational focus in terms of commitment and leadership of senior management, and the involvement, empowerment and training of employees are crucial to inspire a quality culture throughout the organisation, thus contribute to improve quality. The bottom line in this respect is that senior management realises that the long-term benefits of quality far exceed the costs of conformance. Since security is a problem for the whole organisation, it simply is no longer effective or acceptable to manage it from security department. A total approach is what needed in addressing the security problems [1]. Like quality, the key to success in implementing security measures is the commitment and support from senior management so as to inspire the security culture throughout the organisations, thus promote the involvement and empowerment of all employees in security matters.

2.4 Continuous security improvement

Continuous improvement has been proved to be a fundamental for success in quality management, especially in TQM. Since quality improvement is a process, organisations should strive for continuous efforts so as to drive all variability out of the process and achieve a ‘zero defect’ quality goal. The PDCA

(Plan-Do-Check-Act) cycle, commonly known as the Deming cycle, forms the conceptual basis of continuous improvement activities in many companies [3]. Since security is a process and not a product, same approach should also be taken to effectively manage security, meaning that organisations have to strive for continuous security improvement (CSI). This is based on the fact that security threats are not static, and therefore all necessary activities prepared to cope with them should also be dynamic. The CSI cycle would begin with the planning, in which security threats are identified and their criticality and likelihood are determined, vulnerability is assessed and priority is assigned. The next stage is to develop, evaluate, and implement security policy, strategies, and plans to prevent and mitigate the effects of security breaches. As some security breaches may occur, the next step is to verify whether policy, strategies and plans implemented have successfully prevented or mitigated the impacts of successful security incidents, as well as collect additional information from these incidents for further adjustment in the security risk assessment. The next stage of the cycle is to take action, e.g. proper adjustments are conducted so as to complete the security management cycle. From this moment, a new management cycle is taken place, taking into consideration all new inputs from previous steps. The cycle will thus continue and become more and more fine-tuned for a better security management. The CSI cycle is illustrated in figure 1.

Insert Figure 1 about here

3. Risk-based security management (RM) and Business Continuity Management (BCM)

Since security is a component of the organisation’s risk portfolio, it is argued that the management of security should be based on sound risk management, and business continuity should also be one of the expected outcomes of security management. It is emphasised that the benefits of risk-based security management, especially highlighting areas where greater (or lesser) security is needed through the security risk identification, analysis and evaluation [4]. It is also argued that that a stable and reliable port bring risks under control, and that policies aimed at fighting terrorism should be clearly linked with other and existing initiatives aimed at fighting organised crime, piracy, fraud, smuggling, illegal immigration [5]. A detailed study of vulnerability, criticality (consequence) and threat is necessary to formulate a security risk profile. It is argued that such a security risk assessment is the key to making IMO's ISPS Code effective.

A risk-based security management process should consist of four core elements: threat identification, risk assessment, acceptance criteria, and implementation process of risk control. These are clearly the necessary steps of risk management process so as to effectively manage security risks in maritime transport. Specifically, Iarossi [6] and Nolan [7] argue that an effective risk based security management process must take a holistic approach. There are three phases that must be considered within such an integrated process. First, it is necessary to identify all possible threat scenarios. Then the risk of each scenario must be characterised (the threat of each scenario must be assessed, the vulnerability must be analysed, possible consequences of each scenario must be determined). Finally, the information gained from this security risk assessment must be used to adjust the planned risk management controls that are already in place or that should be developed to address normal operation risk. This is in line with John [8] who emphasises that the first step in preventing or minimising the damage caused by disasters or attack is assessment of the risks to the transportation system. Risk assessment is a systematic, analytical process to identify hazards, establish their likelihood, and assess potential severity of a successful attack on some elements of the system. A prioritised, risk-based approach to security management is a critical element to determining practical and affordable solutions. Once the risks are identified, assessed, and prioritised, action plans can be developed to mitigate the risks.

The organisation, in conducting risk management processes, should also communicate and consult them with its internal and external stakeholders. Moreover, these processes need to be continuously monitored and reviewed so as to provide new inputs to keep security management abreast of changing security threats and their probability of occurrence, and therefore, be valid and effective. In addition, the organisation should also address business continuity management as an integral part of its security management, and has in place necessary processes and procedures so that it can return to resilience once a security breach is successful. With all of these in mind, one can argue that the RM approach to security management and consideration of its relationship with BCM would be powerful management weapons for the organisation in the quest of achieving its goals and objectives.

3.1 Conceptual model of effective maritime security

The following model of effective maritime security, consisting of 13 dimensions and 24 associated critical success factors (CSFs), is derived from the QM, RM and BCM approaches discussed above.

Well-structured security policy

(1) Well defined and clear security accountability and responsibility at all levels of the organisation (CSF1)

(2) Documented security processes and procedures (CSF2)

Security risk assessment

(3) Security threats, critical resources to be secured and impacts of successful security threats identified, analysed and evaluated (CSF3)

(4) Minimum security requirements for resources to be secured and risk acceptance level established (CSF4)

(5) Security risk levels clearly defined (CSF5)

Risk-based security mitigation strategies and plans

(6) Security risk mitigation strategies and plans in place and clearly understood by operators (CSF6)

(7) Resource allocation plan to mitigate security risks based on security risk levels (CSF7)

Communication and consultation with stakeholders

(8) Contributions of employees, business partners and related agencies to security policy, strategies, and plans taken as essential inputs (CSF8)

Security monitoring and review

(9) Emphasis of monitoring and review in all security processes and procedures, at all organisational levels (CSF9)

Continuous security improvement

(10) Continuous review and improvement of security policy, strategies, plans, processes and procedures (CSF10)

(11) Use of specific organisational structures (security improvement committee, work teams) to support security improvement (CSF11)

Senior management commitment and leadership

(12) Long-term benefits of security recognised by senior management executives (CSF12)

(13) Security policy, strategies and plans actively directed by senior management executives (CSF13)

(14) Allocation of adequate resources to security improvement efforts, including training (CSF14)

(15) Preparedness of the senior management executives to remove the root causes of security problems (CSF15)

Employee empowerment

(16) Employees encouraged to find and provide feedback on security problems (CSF16)

Employee involvement

(17) Employee involvement in design and planning of security policy, strategies, and plans (CSF17)

Security training

(18) Security training viewed as long-term investment and service quality improvement facilitator (CSF18)

Security design and process control

(19) Security policy, strategies, and plans integrated in overall business policy, strategies, and plans (CSF19)

(20) Security processes and procedures integrated in daily operation processes and procedures (CSF20)

Holistic approach

(21) Technology-based solutions to security problems understood by senior management as not the only answer (CSF21)

(22) Security of information viewed as important as security of physical resources (assets, people, etc.) (CSF22)

Security incident handling and response

(23) Availability of detailed contingency plans to follow in the event of security breaches or incidents, continuously reviewed and updated (CSF23)

(24) Availability of detailed recovery plans to return resilience after security breaches or incidents (CSF24)

4. Research methodology

4.1 Research question and hypothesis

This study aims to examine the research question of what critical success factors for the effective management of security in maritime transport service-providing organisations are. Discussions from the earlier sections have come up with an effective maritime security model of 13 dimensions and 24 factors. The research hypothesis is thus formulated as follows:

> *H_1: Effective maritime security is a construct of 24 identified factors associated with 13 groups of well-structured security policy, security risk assessment, risk-based security mitigation strategies and plans, communication and consultation with stakeholders, security monitoring and review, continuous security improvement, senior management commitment and leadership, employee empowerment, employee involvement, security training, security design and process control, holistic approach, and incident handling and response.*

4.2 Methods of data collection

Triangulation is utilised in this study. Triangulation is strongly suggested in transportation and logistics research literature as an effective and useful technique to achieve the width and depth of research issues [9]. The type of triangulation technique employed in this paper is the methodological triangulation, in which the author uses and combines quantitative and qualitative methods to obtain a comprehensive understanding and a wide and deep picture of the study. The methods of data collection and interpretation used in this study are the survey method (by using mail questionnaires) followed by confirmatory in-depth interviews.

4.3 Sampling design

The sampling frame for this research is constructed from the directory of shipping companies, port operators and freight forwarders/NVOCCs in Vietnam listed in the *Visaba Times—Vietnam Shipping and Logistics Review*. A list of 197 maritime transport service-providing organisations including 66 shipping companies, 49 port operators and 82 freight forwarders/NVOCCs, is used as the mailing list for this research. By the cut-off date, there were 119 returned questionnaires, including 42 from shipping companies, 43 from port operators, and 34 from freight forwarders. This represents a 60% response rate. For the in-depth interviews, it was decided that the same population and sampling frame should be used as for the survey. The process of selecting the samples for interviews was conducted carefully. First, the samples for interviews should be chosen only from within the respondents to these surveys. Secondly, since the research population consists of three categories of service providers, it is important that the sample chosen for qualitative research also reflect the representativeness of these categories. Geographical representativeness of the sample also needs to be assured. As the shipping companies, port operators and freight forwarders/NVOCCs are located all over the North, Central and Southern regions of Vietnam, the sample selected for in-depth interviews should also cover organisations in all these three regions. With these considerations in mind, 25 in-depth interviews were conducted during the study period.

4.4 Design of research instruments

Both fixed-alternative and open-ended response questions were utilised in the questionnaire, preceded by a cover letter using the letterhead of the author's institution. There are two questions in the questionnaire. In the first question, respondents were asked to rate the perceived importance of the 24 critical success factor of effective maritime security on a five-point categorical scale (from 1 indicating not at all important to 5 indicating very important). These items were randomly placed in the questionnaire so as to avoid the order bias. The second question is open-ended, encouraging respondents to supplement and rate any other critical success factor in their business sectors which were not listed in the first question. The questionnaire was originally written in English but later translated into Vietnamese. To ensure that the translation of the instrument in the target language is equivalent to the original language in which the instrument was developed, the process of translation of survey instruments was conducted through the consecutive stages of *forward translation* (English to Vietnamese), *pre-testing* (for both English and Vietnamese versions), *modified translation* (with feedback from instrument pre-testing), *backward translation* (modified Vietnamese version to English), and *finalisation of Vietnamese version* (based on comparison between backward translated English version and the original one).

Since the in-depth interviews aimed at prospective interviewees holding managerial positions, or 'elites', formal questionnaire-based interviews are not appropriate; instead, interviewees are given a great deal of freedom in explaining their answers to pre-determined topics. This means that the same topics, specifically in the form of some open-ended questions, were introduced in each interview but the sequence of questions asked changed over time from one interview to another, and the responses to these questions were in different orders and presented in different ways in different interviews. Moreover, some additional questions beyond the preliminary ones in order to follow-up and probe the interviewee's answers were also asked depending on the specific context in each interview.

4.5 Administering mail survey and conducting in-depth interviews

The questionnaire was pre-tested with a group of 10 organisations selected based on the author's judgement. Once this was completed and all feedback was incorporated to revise the questionnaire, the Vietnamese version of the questionnaire was put in envelopes, together with the cover letter and self-addressed envelopes for returning the answers. A range of various tactics were employed to increase the response rate, such as using the cover letter from the author's institution, carefully phrasing the title of the questionnaire, applying personalisation and anonymity rule, etc.

Prior to the interviews, a list of prospective interviewees in various organisations was worked out, and each of these interviewees was contacted by telephone inviting their participation in the interviews. The list of prospective questions was also forwarded to those who agreed to participate in the interviews. The interviews were conducted on a one-to-one basis between the author and the interviewee, and varied approximately from forty-five minutes to one hour and fifteen minutes. A tape recorder was used to record the whole interview with the prior consent of the interviewees.

5. Findings and discussion

4.1 Measurement scale reliability analysis

In this study, the statistical norm concerning the internal consistency adopted is above ± 2.0, and the accepted value level of reliability (Chronbach's alpha value) is above 0.60 for the scale. Table 1 shows the item-total correlation analysis and Chronbach's alpha value of the scale measuring perceptions of 24 critical success factors. Since all the values in the 'Corrected item-total correlation' column , which shows the internal consistency of the whole scale, are above ± 2.0 (the lowest item has an item-total correlation of 0.3080), it is decided that no variable is dropped from the scale, as each is considered a reliable item measuring effective maritime security. Even when the variable with the lowest item-total correlation is dropped from the scale, the scale's alpha is still very high (0.9238). The overall alpha value for the questionnaire is 0.9229, which indicates that the survey instrument is very reliable.

Insert Table 1 about here

5.2 Perceptions of the proposed critical success factors

Table 2 shows the descriptive statistics data regarding perceptions of respondents in the survey of 24 critical success factors of effective maritime security. A test of significance using Z test [10] was also conducted to test the hypothesis.

Insert Table 2 about here

As can be seen from Table 2, the null hypothesis for all factors is rejected (since z observation values are all greater than z statistics values at 95% confidence level), which means the alternative hypothesis is supported. This is also true at 99% confidence level (z statistics is 2.57). All 24 proposed critical success factors have response mean scores above the midpoint of the scale, thus indicating that all of them are accepted and perceived as critical success factors of effective maritime security. Critically speaking, among the 24 factors, 17 have response mean scores greater than 4, indicating that they are perceived as 'important', while the mean scores of respondents' responses to the remaining factors are greater than 3 but less than 4, showing a lesser magnitude of perceived importance. Nevertheless, it is clear that no factor should be dropped from the scale, and all are valid as critical success factors of effective maritime security.

Respondents rate the *availability of detailed contingency plans to follows in the event of security breaches or incidents with continuous review and update* (CSF23) as the most important factor. Another factor relating to how organisations handle and respond to security incidents, *availability of detailed recovery plans to maintain business resilience after security breaches or incidents* (CSF24), is also highly rated as the third most important factor. It is clear that respondents highly appreciate factors relating to how the organisation prepares to continue its business after a security incident. Moreover, it is emphasised that these factors are closely connected to quality management, as the contingency and recovery plans should be continuously reviewed and updated. There is also a very high level of consensus in the interviews among all informants who agree on some common reasons that organisations should have in place a detailed contingency plan to respond to materialised security risks, as well as a plan to restore business operations. All informants highly appreciate the importance of business continuity, as business performance is the ultimate objective of organisations, and thus security needs to serve this objective as well. As a result, no matter what happens, it is critical that organisations respond effectively to materialised risks to minimise their consequences, as well as maintain business resilience. The main reason behind the informants' argument is that, while it is necessary to assess risks in advance, not all risks can be identified and prevented, and when breaches actually happen there will be no time for thinking what to do. Moreover, it is also critical for organisations to continue their business after the incident, to survive and grow. It is therefore argued by the informants that contingency plans should be included in the security policy and plans in advance, continually reviewed and updated, as well as constantly practised. Such plans would therefore contribute to make security management more effective. Some informants even argue that how managers handle a crisis situation would demonstrate their capability. Clearly, not only in service quality but also in security management, incident handling capability is highly appreciated together with plans to build this capability. Indeed, while organisations may rarely implement such plans, their preparation in advance and frequent practise are critical to ensure that the organisation effectively mitigates risks and continues their business as usual. The following comment of a ship operator best summarises this perception:

> '… Nobody can deny that when a security incident occurs, there will be absolutely no time to think what to do, no time to organise works if everything is not planned beforehand, so those security plans with details of mitigation and business continuity strategies are extremely important'.

Factors relating to security policy are also highly rated by the respondents. In this respect, the second most important factor is *documented security processes and procedures* (CSF2). Respondents also emphasise the importance of *well-defined and clear security accountability and responsibility at all levels of the organisation* (CSF1), as this factor is rated as the sixth most important critical success factor. It is clear that a well-structured security policy plays an important role and is a critical element of good security management. In much of the literature, it has been argued that effective maritime security should start with the security policy. Specifically, the policy should be well-structured, e.g. clear, documented, easy for all employees to understand and implement, etc. Such a security policy lays the foundation for effective maritime security since without it all other security plans, processes and procedures may not be devised and implemented properly. Moreover, such a security policy will ensure that employees do not merely pay lip-service to it, but rather make it part of their daily business and implement it voluntarily. In this connection, although some informants express the view that such a policy is not necessary for some small organisations with limited financial resources, most informants show a high consensus on the issue as a factor in effective maritime security. This perception is seen across ship and port operators and freight forwarders/NVOCCs.

As expected, factors involving security risk assessment and risk-based security mitigation strategies and plans are also perceived as being among the most important critical success factors of effective maritime security. In this connection, respondents view *security risk levels clearly defined* (CSF5), *resource allocation plan to mitigate security risks based on defined security risk levels* (CSF7), *minimum security requirements for resources identified and risk acceptance level established* (CSF4), *security threats, critical resources to be secured and impacts of security threats identified, analysed and evaluated* (CSF3), *security risk mitigation strategies and plans should be in place and clearly understood by operators* (CSF6), as the fourth, the eighth, the ninth, the tenth, and the thirteenth most important factor respectively. It is also evident from the interviews that informants highly appreciate risk assessment for any security measures to be introduced and implemented. Basically, the main rationale for this is prevention is always better than waiting for something to happen and then reacting to it, so the analysis and assessment of potential risks in advance, then formulation and implementation of security policy, strategies and plans based on them, would lead to effective maritime security. Another argument is that without risk assessment, companies may not realise the different levels of various security risks and thus may not be able to have an appropriate security policy, strategies and plans to cope with them effectively. To many informants, it is critical to balance the use of limited resources for both security and business objectives, as well as better identify which security risks organisations can bear themselves and which should be transferred to another party. Other informants argue that as security risks are part of business risks, their identification and assessment should be conducted as part of the overall identification and assessment of the company's risk profile. The following comment of an informant working in a shipping company further elaborates this perception about security risk assessment:

> '…If you want to implement security measures in the long term and frequently, you should review possible security risks and assess their potential impacts… This assessment is very important, in my opinion, since we can base on that to foresee bigger possible consequences for the company… With the assessment, we can devise proper detailed measures in specific scenarios. So I think that is absolutely necessary when the company wants to formulate their security policy'.

In any management issues, the role of senior management is very important, as they need to take the lead and be involved in these issues to set an example for their staff. This is proved in many studies about quality management and is expected to be applicable in security management as well. Indeed, factors relating to senior management commitment and leadership are also highly rated in this study. Specifically, *allocation of adequate resources to security improvement efforts, including training* (CSF14), *security policy, strategies and plans actively directed by senior management executives* (CSF13), *senior management executives recognise the long-term benefits of security* (CSF12), *preparedness of senior management executives to remove the root causes of security problems* (CSF15) are ranked the fifth, the seventh, the eleventh, and the sixteenth most important factors respectively. The role of senior management commitment and leadership is least controversial in all interviews since all informants perceive it as a prerequisite for security management, and argue that security management is only effective with the highest level of involvement and leadership of the senior management executives. The informants' main rationale is that senior management executives are at the highest level of management of the organisation, so if the security policy does not receive their due concern it will be just a paper only and cannot be operational. Because of their position, senior management executives are also the first to realise the importance of risk prevention and mitigation. They have to be involved and take leadership in every management matter, including security management, provide proper guidance in formulating security policy, strategies, and plans, and necessary support for employees, to complete their job successfully. Many informants concern that the role of senior management is very critical, since they have to be fully aware about and take security management seriously and hence inspire their employees. If no set example is set by senior management, employees will tend to pay lip-service only to security. Another argument is that senior management executives play an important role in creating the working environment and culture in which everybody, from the senior managers to general employees, all voluntarily comply with security requirements and practices. This role of senior management is especially emphasised in many interviews, summarised by a ship operator as follows:

> ‘As the highest level of management, the senior management should take issues of safety, security and environment protection seriously, otherwise they cannot set example and encourage their employees to do so. They have to organise, take leadership, and provide necessary assistance and support so that employees can do their daily jobs as well as security practices well. The senior management also have to provide education and training for employees so that the security awareness can be inspired in the whole company’.

In achieving effective maritime security, factors involving security design and process control are also appreciated by the respondents. Specifically, *security processes and procedures should be integrated in daily operation processes and procedures* (CSF20), and *security policy, strategies and plans should be integrated in overall business policy, strategies and plans* (CSF19) are ranked the twelfth and the fourteenth most important factor respectively. There is also a high level of consensus among interview informants towards these factors. There are some common main reasons for the informants’ arguments. Firstly, it is agreed that security risks, like other risks in the business environment, are always changing and so is their probability of occurrence. If the security policy, strategies, plans, processes and procedures are static they will soon not be able to keep up with the changes of security risks and thus will no longer be realistic and effective. It is therefore important that organisations continuously review, update and improve them. Secondly, informants argue that security is part of the business practices and thus should be incorporated into the overall business practices for a holistic view of the management and implementation. Such an integration will also facilitate the security functions and encourage employees to take security into account rather than pay lip-service to it. They strongly argue that if security is separated from the overall business, it may be conducted merely as a reaction to legal and social regulations, or just a matter of paperwork. The integration will also mean better and more efficient coordination between security and business plans. An informant working in a port operation company comments on this issue as follows:

> '… If security is separated from the operations activities, they will have a separate view of the business and thus cannot fully support them… Security should be closely linked with business activities, because the outcomes of security are part of the service the port provides its customers'.

Beyond security and process control, respondents also focus on factors involving communication and consultation with stakeholders as a critical success factor of effective maritime security. In this connection, it is confirmed by respondents that *contributions of employees, business partners and related agencies to security policy, strategies and plans, including their changes if any, incorporated as essential inputs* (CSF8). This factor is ranked fifteenth in importance. As far as interview informants are concerned, most of them argue that the communication about and consultation on security issues with the company's stakeholders is also essential to effective maritime security. However, not all informants agree about this issue. From the 25 informants, two do not quite agree with the general perception, reasoning that if security plans, processes and procedures are disclosed to stakeholders they are no longer security. However, they agree that to obtain security information from stakeholders, but not communicate to them, is very necessary. The majority of informants, on the other hand, argue that it is critical to communicate with and consult stakeholders on security issues. Such activities help the organisations to update in line with changes in the overall socio-economic situation related to security through their business and social partners, because there is much security information that the company cannot acquire themselves but which can be seen very clearly by external partners. Moreover, it is also agreed that security information collected and analysed from various sources is always better than from a single source, and it is a better basis on which organisations can devise appropriate security measures. A port operator elaborates this perception as follows:

> ‘If we can consult from our vendors, or other related agencies such as customs, coast guard, port authority, local police, etc. we can obtain holistic and objective information to devise possible scenarios, thus formulating suitable policy, strategies and plans. Such a formulation should not be based on the subjective judgement of the company alone, but should be on the synthesis and analysis of collected information from various sources. They will help the company in devising the most realistic possible security measures for prevention as well as mitigation’.

It is affirmed by the respondents that, in dealing with maritime security threats and achieving their effective management, organisations should also have a holistic approach in that *security of information should be viewed as important as security of physical resources* (CSF22) and senior management should understood that *technology-based solutions to security problems are not the only answer* (CSF21), those are ranked the seventeenth and the twenty-first most important factors. Respondents also agree that *employees should be encouraged to find and provide feedback on security problems* (CSF16) as this factor is rated eighteenth in importance. Clearly, as in quality management, employees should be empowered to bright their jobs and make security management more effective. Interview informants also concur with survey respondents in this respect. Specifically, informants were asked to provide their views and comments on whether technology-based solutions to security problems would be the most important and appropriate. This is to explore their perceptions of how the security management issue should be approached, e.g. considering it as a technology-driven or a business-driven issue which should therefore be viewed from a holistic perspective. Interestingly, all the informants, while acknowledging that technology-based solutions are becoming more and more important to security management, believe that they are not the most important and sole solutions to the issue. Instead, they affirm the critical importance of the human factor, specifically the security awareness of senior management executives and employees, as well as the appropriate planning and implementation of security policy, plans, processes and procedures. There are some arguments for this perception. Firstly, it is argued that technology solutions, no matter how sophisticated they are, are created by people and thus they can also be cracked or manipulated for criminal purposes by people. Moreover, if the operators of such technology solutions do not have high security awareness they cannot effectively utilise these technology solutions. Secondly, technology solutions should be accompanied by appropriate planning and effective implementation of security processes and procedures based on risk assessment principles. Otherwise, they could hinder the smooth flow of business processes. It is evident that, in security management and improvement, the role of people is extremely important, as people create technology as well as policy, processes and procedures. If people have high security awareness and good training, they can, together with technology, improve security while enhancing business processes at the same time. The following comment from a port operator illustrates these arguments.

> 'I do not think technology is the unique and most important factor in security improvement; rather security improvement should be based firstly on the improvement of procedures and increase of security awareness… Of course, technology is more and more important in the next decades. If the company has better resources, especially financial strength, they can invest more on modern and sophisticated technology to enhance security. Technology is just assisting the human beings to do their jobs better'.

Factors relating to continuous security improvement are also perceived by the respondents as being important inputs to effective maritime security. In this connection, *continuous review and improvement of security policy, strategies, plans, processes and procedures* (CSF10) is rated as nineteenth in importance. Meanwhile, *use of specific organisational structures to support security improvement* (CSF11) is ranked at twenty-third in the list of critical success factors of effective maritime security. For security management to be effective, respondents also agree that there should be *emphasis on monitoring and review in all security processes and procedures, at all organisational levels* (CSF9). This is ranked twentieth in the list of factors. There is also consensus on security training, as *security training viewed as long-term investment and service quality improvement facilitator* (CSF18) is ranked as the twenty-second most important critical success factor of effective maritime security.

The least important critical success factor as perceived by the respondents is *employee involvement in design and planning of security polity, strategies and plans* (CSF17). This magnitude of importance may be explained as follows: although *employees should be encouraged to find and provide feedback on security problems* (CSF16), the design and planning of security policy, strategies and plans require specialised staff expertise and skills for which general employees may not be qualified. Relating to this issue, informants strongly argue that employees play an important role in security management since they are at the operational level and directly implement security policy, plans, processes and procedures. Senior management executives devise security policy, plans, processes and procedures, but it is employees who implement them, and thus interact on a daily basis with security problems in their daily work. It is therefore reasonable that employees should be encouraged to identify security loopholes and contribute ideas to solve security problems. This is also considered an empowerment of employees, since such encouragement for them to be involved in security improvement activities would give them the feeling of being worthy of greater responsibility and being part of the whole company process. That, in turn, will encourage them to be better and more effective in their jobs.

6. Implications, limitations and direction for future research

6.1 Academic implications

This research has several academic implications. Firstly, it helps fill the gap in the literature about effective maritime security, as it has been identified earlier that there has been very few studies conducted in this field. Secondly, this study utilises the triangulation of theories on quality, risk, and business continuity management to propose and validate the model, thus provides insights on maritime security management. Thirdly, although the model of effective maritime security in this research was designed and tested specifically with a group of maritime transport organisations, its application could be generalised to other service sectors. Although the model in this study has factors dedicated to maritime transport, its 13 dimensions are rooted in and built from general quality and risk management literature. Researchers with interest in security management in other business sectors can use this model's dimensions as a general framework model while individual factors within each dimension can be developed tailor-made to each specific sector. To this end, the model developed and tested in this research is of contribution to enrich both generic and maritime transport security management literature.

6.2 Managerial implications

The managerial implications of this research are two-fold. Firstly, as it has never been a universal approach to evaluating how security can be effectively managed in maritime transport sector, this research provides managers in maritime transport organisations a useful tool for that purpose. Managers can use the model designed and tested in this research to develop a checklist of essential components for their company's security management policies, strategies, and plans. The use of a universal checklist by maritime transport organisations to evaluate their maritime security management would also greatly facilitate benchmarking across organisations in the industry, as the same metrics is used. This, in turn, would enhance the image of the industry as a whole. Secondly, the ranking of factors in this research, though is of reference only to managers as it has just been tested in a single country, would provide insights to areas of security management which should be focused upon.

6.3 Limitations and direction for future research

This research has a major limitation, which is that it has just been conducted in one country. Future research direction is desired, e.g. conducting the study using the same instruments in various countries with different socio-economic settings so as to enhance the reliability and validity of this study's findings.

7. Conclusion

This paper reviews the concept of effective maritime security, and specifically aims at devising and empirically testing a conceptual model of effective security management in maritime transport, which is derived from the quality, risk and business continuity management approaches. A synthesis from this perspective has led to a proposal of a effective maritime security model which consists of 13 dimensions, *well-structured security policy*, *security risk assessment*, *risk-based security mitigation strategies and plans*, *communication and consultation with stakeholders*, *security monitoring and review*, *continuous security improvement*, *senior management commitment and leadership*, *employee empowerment*, *employee involvement*, *security training*, *security design and process control*, *holistic approach*, and *incident handling and response*, further explained by associated 24 factors. Through analyses and discussions of empirical findings, it has been evident that the proposed model is verified by both survey respondents and interview informants. Specifically, factors involving security incident handling and response are rated as the most important in magnitude, along with security risk assessment, risk-based security mitigation strategies and plans, and senior management commitment and leadership. This finding supports the suggested model of effective maritime security, in which maritime security management could be effective by practising factors derived from quality, risk, and business continuity management approaches. Managers in maritime transport organisations can use the model designed and tested in this research to develop a checklist of essential components for their company's security management policies, strategies, and plans. In addition, the use of a universal checklist to evaluate maritime security management would also greatly facilitate benchmarking across organisations in the industry and thus enhance image of the industry as a whole. While the maritime effective security model in this research provides some contribution to related literature and management practice, it can be further conducted using the same instruments in various countries with different socio-economic settings. This aims to enhance the validity and reliability of this research's instruments and findings.

References

[1] LEE, H. L. and WHANG, S., 2003, Higher supply chain security with lower cost: lessons from Total Quality Management, http://gobi.stanford.edu/ResearchPapers/Library/RP1824.pdf.

[2] LEE H. L. and WOLFE, M., 2003, Supply chain security without tears, http://www.manufacturing.net/scm/index.asp?layout=articlePrint&articleID=CA278114.

[3] DEMING, W. E., 1986, *Out of the crisis* (Cambridge, MA: MIT Technology Centre for Advanced Engineering Study).

[4] BRODER, J. F., 1984, *Risk analysis and the security survey* (USA: Butterworth Publishers).

[5] ESPO, 2002, Port and maritime security, www.espo.be/policy/initialviewsFINAL.pdf.

[6] IAROSSI, F, J., 2002, Creating a safe and secure environment for the marine transportation of energy, http://www.absconsulting.com/news/fji-nov182002.html.

[7] NOLAN, T. M., 2003, Security and safety: real responses to maritime security threats, www.socp.org/archive/3-5-03/presentation-3-5-03/tn_abs.ppt.

[8] JOHN, A., 2003, Risk assessment and prioritisation. *Volpe national transportation systems centre*, http://www.volpe.dot.gov/infosrc/journal/2003/pdfs/chap1.pdf.

[9] CUNNINGHAM, L., YOUNG, C. & LEE, M., 2000, Methodological Triangulation in Measuring Public Transportation Service Quality. *Transportation Journal*, **Fall**, 35–47.

[10] ZIKMUND, W., 2003, *Business Research Methods*, 7th edition (USA: Thomson Learning, South-Western Publishers).

FIGURES AND TABLES

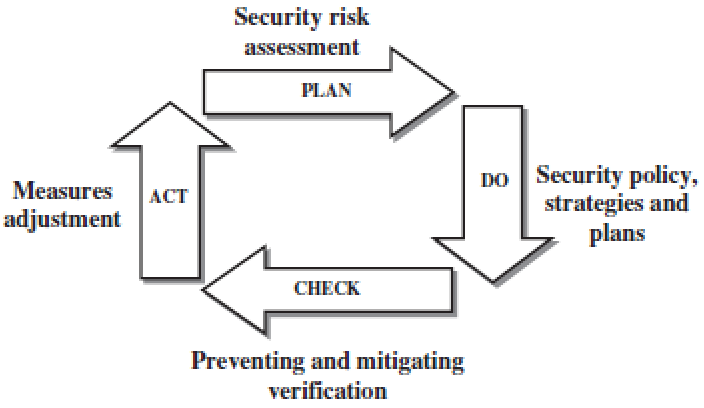
Security risk assessment
PLAN
DO
Security policy, strategies and plans
CHECK
Preventing and mitigating verification
ACT
Measures adjustment

Figure 1: The Continuous Security Improvement (CSI) cycle

Alpha = 0.9229				
Critical success factors (CSFs)	**Scale mean if item deleted**	**Scale variance if item deleted**	**Corrected item-total correlation**	**Alpha if item deleted**
CSF5	94.6723	73.7476	0.3080	0.9238
CSF20	94.9496	71.2178	0.4323	0.9226
CSF6	94.9580	73.5999	0.4001	0.9222
CSF1	94.6891	72.2161	0.4437	0.9217
CSF24	94.5462	71.9788	0.4538	0.9216
CSF14	94.6891	72.6906	0.4464	0.9215
CSF19	94.9580	70.5999	0.4872	0.9214
CSF8	94.9832	72.6607	0.4989	0.9208
CSF3	94.8571	72.3947	0.5002	0.9207
CSF2	94.5294	71.7428	0.5195	0.9204
CSF4	94.8319	71.9715	0.5548	0.9199
CSF23	94.4538	71.5381	0.5585	0.9198
CSF16	95.1176	71.4267	0.5697	0.9196
CSF7	94.7731	71.3294	0.5671	0.9196
CSF22	95.0924	70.4914	0.5823	0.9193
CSF13	94.7227	71.2699	0.5939	0.9192
CSF11	95.5882	70.7188	0.6410	0.9184
CSF17	95.7647	68.2662	0.6454	0.9182
CSF10	95.2353	69.8425	0.6684	0.9178
CSF12	94.8992	69.1253	0.6592	0.9178
CSF15	95.0924	69.1185	0.6720	0.9176
CSF18	95.4706	69.5902	0.6911	0.9174
CSF21	95.3782	69.2710	0.6910	0.9173
CSF9	95.2605	69.0078	0.7344	0.9165

Table 1: Reliability analysis of scale measuring effective maritime security

Critical Success Factor	Mean	STD	Rank	Z statistics (95% confidence)	Z observation
CSF23	4.66	0.56	1	1.96	32.31
CSF2	4.58	0.57	2	1.96	29.98
CSF24	4.56	0.62	3	1.96	27.53
CSF5	4.44	0.58	4	1.96	27.17
CSF14	4.42	0.54	5	1.96	28.45
CSF1	4.42	0.60	6	1.96	25.67
CSF13	4.39	0.55	7	1.96	27.30
CSF7	4.34	0.57	8	1.96	25.50
CSF4	4.28	0.52	9	1.96	26.82
CSF3	4.25	0.52	10	1.96	26.05
CSF12	4.21	0.69	11	1.96	19.21
CSF20	4.16	0.74	12	1.96	17.18
CSF6	4.15	0.48	13	1.96	26.12
CSF19	4.15	0.73	14	1.96	17.15
CSF8	4.13	0.50	15	1.96	24.73
CSF15	4.02	0.68	16	1.96	16.40
CSF22	4.02	0.64	17	1.96	17.40
CSF16	3.99	0.56	18	1.96	19.32
CSF10	3.87	0.62	19	1.96	15.42
CSF9	3.85	0.63	20	1.96	14.63
CSF21	3.73	0.65	21	1.96	12.33
CSF18	3.64	0.62	22	1.96	11.22
CSF11	3.52	0.57	23	1.96	10.06
CSF17	3.34	0.78	24	1.96	4.85

Table 2: Perception of proposed 24 critical success factors

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