

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

Title	Impacts of Implementation of the Effective Maritime Security Management Model (EMSMM) on Organizational Performance of Shipping Companies
Author(s)	Sadovaya, Elena; Thai, Vinh Van
Citation	Sadovaya, E., & Thai, V. V. (2015). Impacts of Implementation of the Effective Maritime Security Management Model (EMSMM) on Organizational Performance of Shipping Companies. <i>The Asian Journal of Shipping and Logistics</i> , 31(2), 195-215.
Date	2015
URL	http://hdl.handle.net/10220/38712
Rights	© 2015, The Korean Association of Shipping and Logistics, Inc. Production and hosting by Elsevier B.V. All rights Reserved. Peer review under responsibility of the Korean Association of Shipping and Logistics, Inc.

Impacts of Implementation of the Effective Maritime Security Management Model (EMSMM) on Organizational Performance of Shipping Companies*



Elena SADOVAYA ** · Vinh V. THAI ***

Contents

I. Introduction	IV. Analysis and Results
II. Literature Review	V. Findings and Discussion
III. Research Methodology	VI. Conclusion

Abstract

This paper aims to examine the impacts of the Effective Maritime Security Management Model (EMSMM) on organizational performance of shipping companies. For this purpose, a survey was administered to collect data from shipping and ship management companies worldwide. The hypotheses in this study were tested using the structural equation modelling (SEM). It was found that the proposed model has direct positive impacts on security, business resilience and customer performance, as well as indirect positive relationship with security-related, and time market performance. Besides, the categorization of organizational performance of shipping companies, proposed and empirically validated in this study, can be used by the companies to measure the impacts of security management.

Key Words : Maritime Security, Effective Maritime Security Management, Impacts of Security Management, Organizational Performance of Shipping Companies

Copyright © 2015, The Korean Association of Shipping and Logistics, Inc. Production and hosting by Elsevier B.V.
All rights Reserved. Peer review under responsibility of the Korean Association of Shipping and Logistics, Inc.

* This is the revised version of the paper presented at the 7th International Conference on Asian Shipping and Logistics, Seoul, Korea, 30 – 31 October 2014.

** Ph.D. Candidate, Nanyang Technological University, Singapore, Email: elena2@e.ntu.edu.sg

***Assistant Professor, Nanyang Technological University, Singapore, Email: vvthai@ntu.edu.sg

I. Introduction

To enhance maritime security in shipping companies, a number of compulsory and voluntary regulations have been introduced at various levels. However, besides benefits expected from implementation of these regulations, it has also had negative impacts (Thai, 2007; Urciuoli et al., 2010; Yang, 2010). For some companies, additional cost related to security implementation resulted in bankruptcy. Additionally, benefits expected have not been fully obtained (Voss, et al., 2009). Besides, managers do not clearly understand how the introduced security requirements can help in the prevention and recovery from a terrorist attack, since available information about the attacks is very limited (Yang, 2010; Urciuoli, et al., 2010). The misunderstanding about benefits and negative results may jeopardize the implementation of security regulations in shipping companies (Voss, et al., 2009; Yang, 2010). Thus, to manage security effectively, companies need to decide what security initiatives to comply with, how to allocate resources effectively, and how to manage security effectively (Gould, et al., 2010; Hints et al., 2009).

This study therefore has two main objectives. First, it aims to validate an Effective Maritime Security Management Model (EMSMM), which was developed by Sadovaya and Thai (2014) to help shipping companies in effective implementation of compulsory and voluntary security requirements. The second objective is to study the impacts of the proposed model on organizational performance of shipping companies. The remaining of the paper is structured as follows. First, a literature review is conducted, followed by the research methodology, including model building and method of data collection. The analysis and results are then discussed, followed by discussion on the findings and their implications. The final section of the paper provides conclusions and future research suggestions.

II. Literature Review

1. Maritime Security Management (MSM) in Shipping Companies

A number of supply chain and maritime security initiatives have been

introduced by government and industry organisations. Among them are Secure and Facilitate Global Trade (SAFE) Framework of Standards, Secure Trade in the APEC Region (STAR) Initiatives, Singapore Customs Secure Trade Partnership (STP), Business Anti-Smuggling Coalition (BASC) Initiatives. Besides, the ISO Standards provide guidance for security management in companies of the supply chain. However, these programs mostly focus on the implementation of voluntary requirements and do not cover all other applicable security measures.

In the academic literature, the most commonly mentioned management approaches include risk management (Thai and Grewal, 2007; Thai, 2009; Gould, et al., 2010), quality management (Thai and Grewal, 2007; Thai, 2009, 2013; Hintsä, et al., 2009; Gould, et al., 2010; Urciuoli, et al., 2010), business continuity management (Gutiérrez, 2007; Thai, 2009; Gould, et al., 2010; Nevrous, 2010), disaster management (Macdonald and Corsi, 2013), crisis management (Gutiérrez, 2007), layered approach (Bichou et al., 2014; Urciuoli et al., 2010), and total security management. Based on the listed approaches, number frameworks were introduced in the area of maritime and supply chain security management. Among them are the supply chain security management model (SCSMM) developed by Gutiérrez (2007), the framework for supply chain security management (FSCSM) proposed by Closs et al. (2008), the conceptual models of effective maritime security (CMEMS) introduced by Thai (2009), and the maritime security management system (MSMS) proposed by Thai and Grewal (2007). With a detailed consideration of these frameworks, a list of essential criteria for EMSMM was introduced in the study of Sadovaya and Thai (2014). Table 1 lists the criteria and highlights the frameworks for MSM that have addressed these criteria. It also shows that none of the existing frameworks satisfies all of these criteria.

2. The Link between MSM and Organizational Performance

The discussed security management approaches as well as models and systems are expected to help shipping companies in security improvement. However, besides the expected benefits, these initiatives often have negative impacts on organizational performance. The misunderstanding of benefits and negative results may jeopardize the implementation of security regulations (Gould, et al., 2010; Voss, et al., 2009; Williams et al.,

2008; Yang, 2010). Nevertheless, (Bichou et al., 2014, p. 3) argued that “impacts of maritime security still remain under-researched and fragmented”. This section therefore provides a review of literature in order to understand how the implementation and management of security requirements affected or may affect shipping companies’ performance.

<Table 1> List of essential criteria for EMSMM and frameworks satisfying them

<i>Essential Criteria</i>	<i>Frameworks</i>
1. The EMSMM is easily applicable in practice and provides guidance for implementation.	SCSMM (Gutiérrez, 2007) FSCSM (Closs, et al., 2008)
2. The EMSMM helps to implement compulsory and voluntary maritime security requirements.	SCSMM in Gutiérrez (2007)
3. The EMSMM is developed specifically for shipping companies and ports.	MSMS (Thai and Grewal, 2007)
4. The EMSMM aims to achieve the balance between security, efficiency and resilience.	SCSMM (Gutiérrez, 2007)
5. The EMSMM links security management and its impacts on organizational performance.	Partly in SCSMM in Gutiérrez (2007)
6. The EMSMM is based on the holistic approach to security management.	MSMS (Thai and Grewal, 2007) CMEMS (Thai, 2009)
7. The EMSMM is easily adopted by different shipping organizations.	MSMS (Thai and Grewal, 2007) CMEMS (Thai, 2009)

There are many papers focusing mostly on positive impacts (Crutch, 2006; Gutiérrez, et al., 2007; Thai, 2007). Only a few papers discussing negative impacts of security management were found (Bichou, 2008; Urciuoli, et al., 2010; Yang, 2010). Besides, some voluntary programmes, for example, WCO Safe Framework of Standards and Secure Trade Partnership, propose benefits that shipping companies will enjoy if they become participants. However, participating companies do not enjoy all expected benefits (Gutiérrez et al., 2007). It might be explained by a short period of time that passed since the new security regime came into force. To date, not much data were reported on the obtained impacts of maritime security requirements on organizational performances of shipping companies. The lack of data may be associated with the unwillingness of industry representatives to provide the information, because it might negatively impact their reputation. Additionally, there are just a few studies that actually examine the existence of these impacts (Thai, 2007; Gutiérrez et al., 2007; Yang, 2010; Urciuoli, et al., 2010; Voss, et al., 2009). Table 2 shows the classification of impacts.

<Table 2> Impacts of implementation of security requirements on organizational performance of shipping companies

<i>Positive Impacts</i>		<i>Negative Impacts</i>	
<i>Reported</i>	<i>Proposed</i>	<i>Reported</i>	<i>Proposed</i>
<ul style="list-style-type: none"> • increase in revenue (7) • enhanced branding (6,10) • reduce of cost (6) • reduce of insurance cost (6) • reduce of transit time • improved efficiency (7) • improved security: (7,10) <ul style="list-style-type: none"> - reduced pilferage (6) - reduced stowaways (11) - reduced attacks (11) - reduction in tampering - reduction in damages (6) - reduction in smuggling (6) • security awareness (10) • cooperation btw company, port, gov-t • reduced number of inspection • priority for inspection • better governance: <ul style="list-style-type: none"> - better use of IT (10) - better document processing (7,10) - improved cargo handling (7) - improved manpower utilization (7) - improved inventory management (7) - better data management (7) • better problem response (6) • quicker recovery from accidents (6) • customers' satisfaction (7) • higher customer service 	<ul style="list-style-type: none"> • enhanced branding (5,9) • increased competitiveness (5) • reduce of cost (2) • reduce of insurance cost (2) • reduce of transit time (2,4) • improved efficiency (1,9) • increased visibility (2,4,9) • increased liability • improved security: <ul style="list-style-type: none"> - reduced pilferage (1,4,5,9) • cooperation btw company, ports, gov-t (2,8) • reduced number of inspection (4,5,9) • priority for inspection • better governance: (1) <ul style="list-style-type: none"> - better use of IT (1,8) - improved product handling (4) - better data management (2,4) • better problem response(4) 	<ul style="list-style-type: none"> • financial loss (14) • lower competitiveness (14) • reputation injury (14) • additional cost: (10,12,14) <ul style="list-style-type: none"> - higher salary (12) • longer process time: (12,14) <ul style="list-style-type: none"> - delays in container clearance (10,14) - congestions (14) • less reliability (12) • less flexibility (12,14) • risk of disclosure of sensitive information (14) • need for extra staff (10) • staff shore leave (11, 15) • extra workload (10,14) • security taxes, tariffs 	<ul style="list-style-type: none"> • lower competitiveness • additional cost: (1,2,8) <ul style="list-style-type: none"> - increase insurance premiums • longer process time: (1,2,8) <ul style="list-style-type: none"> - delays in container clearance (1,3,8) - congestions • need to share the information with gov-t (1,13) • risk of disclosure of sensitive information (3) • need for staff training (1) • security taxes, tariffs (8) • decline of late bookings (2)

Note: numbers in brackets indicate following publications: 1, 2, Bichou (2008); 3, Bryant (2009); 4, Crutch (2006); 5, 6, Gutiérrez et al. (2007); 7, 8, 9, 10, Thai (2007); 11, Timlen (2007); 12, Urciuoli et al. (2010); 13, Voss et al. (2009); 14, Yang (2010); 15, Goulielmosa et al., (2014).

As can be seen from Table 2, not all of the proposed impacts were found among the reported. Besides, the implementation of security requirements has unexpected negative impacts. The significant difference in the obtained results may be explained by the fact that the same security requirements are implemented in different ways by shipping companies. That is why the effective MSM in shipping companies is an essential condition for achieving benefits and avoiding negative impacts (Gould, et al., 2010; Gutiérrez, 2007; Thai, 2007). To contribute to the understanding of the effective MSM, the link between security management in shipping companies and their organizational performance is studied in this paper.

3. Organizational Performance of Shipping Companies

The literature on organizational performance reviewed in this section is organized into two groups. The first group includes papers studying organizational performance in a general context and a context of supply chain, but not related to security. As shown in Table 3, there are four most common categories of organizational performance. The categories' names might vary, however the performance indicators are the same. The second group of the literature combines papers on impacts of MSM on organizational performance. The categorization from Table 3 was used in one of the studies from the second group, conducted by Williams (2008) on outcomes of supply chain security. Whereas, the other studies from the second group mostly focus on internal business performance and customer performance. In most cases, however, the security and safety indicators representing internal business performance are not detailed enough to measure improvements in these areas.

Nevertheless, there are few studies found where security and resilience indicators were grouped in separate categories (Crutch, 2006; Gutiérrez et al., 2007). However, the lists of indicators presented in these studies are not comprehensive enough in comparison with those shown in Table 2, and, therefore, cannot fully measure impacts on security, resilience and other organizational performance. Therefore, a comprehensive list of organizational performance needs to be further developed for a purpose to measure these impacts. Besides, there is a clear need for more information and research on the reported impacts of MSM on organizational performance of shipping companies.

<Table 3> Categories of organizational performance found in the literature

<i>Category of organizational performance</i>	<i>Performance indicators</i>	<i>Sources</i>	
		<i>General studies</i>	<i>Studies on SC and maritime security</i>
Financial performance/ Firm performance	profit, ROI, ROA, return on sale, profitability, cash flow, profit-to-revenue ratio	Evans (2007), González-Benito (2007), Feng et al. (2008), Green et al. (2008)	Williams (2008)
Market performance/ Marketing performance/ Commercial performance	market share, market growth, sales volume, sales growth, market development, new product/service development, competitive position, reputation and image, access to global market;	Evans (2007); González-Benito (2007); Feng et al. (2008); Green et al. (2008).	Williams (2008)
Operational performance/ Manufacturing performance/ Internal business performance/ Supply chain performance/ Logistics performance/ Quality outcomes	quality (service, product), cost, productivity, flexibility, reliability (dependability), visibility, delivery speed, transit time, delivery failure, employee turnover, efficiency, response time, defect rate, variety of service, shipment accuracy, internal procedures, employee morale, resilience, safety, risk, security.	Feng et al. (2008); Green et al. (2008).	Thai (2007); Williams (2008); Urciuoli et al. (2010).
Customer performance	customer relationship, customer satisfaction, number of customer contact points, customer retention rate, customer commitment, knowledge of customers' needs	Evans (2007).	Thai (2007); Williams (2008).

Source: authors, adapted from various sources

III. Research Methodology

1. Model Building

The effective maritime security management model (EMSMM), adopted from Sadovaya and Thai (2014), contains nine factors and 53 associated attributes, as shown in Figure 1. To validate the model, a face validity test, an exploratory and confirmatory factor analyses (EFA and CFA) were conducted first. Next, the indicators of organizational performance of shipping companies were classified into three categories, namely Security Performance, Business Resilience and Other Business

Performance, as shown in Figure 2. This classification was chosen, since one of the essential criteria for the EMSMM is to achieve a balance between security, resilience and efficiency in shipping companies. Even though, the proposed categories cover the performance indicators from Table 3, the classification is unique and therefore should be validated through a face validity test, the EFA and CFA. With a consideration of the discussed classification, the main hypotheses was formulated as follows:

Hypothesis 1: The EMSMM positively impacts Security Performance of shipping companies.

Hypothesis 2: The EMSMM positively impacts Business Resilience of shipping companies.

Hypothesis 3: The EMSMM positively impacts Other Business Performance of shipping companies.

2. Data Collection

A survey questionnaire, containing two main questions, was employed. Respondents were asked to indicate their agreement with each attribute of the EMSMM, as listed in Figure 1, regarding security management in their companies. A 5-point Likert Scale ranging from 1 (strongly disagree) to 5 (strongly agree) was applied. The second question was about changes in organizational performance of participating companies. For this question, performance indicators, listed in Figure 2, was measured by a 5-point scale, where 1 represents “significantly decrease” and 5 – “significantly increase”. To test the face validity of the items, a pre-test with 19 academics and industry professionals in Singapore was conducted.

The study population of the survey consists of shipping and ship management companies worldwide, listed in the Seaweb database. The stratified sampling method was applied to compose the mailing list. Information about 46,871 companies was extracted from the database in accordance with world’s regions grouping, suggested by the United Nations. Then, to reduce the sampling size, 90% of population was dropped, resulting in 4,687 companies.

Impacts of Implementation of the Effective Maritime Security Management Model (EMSMM) on Organizational Performance of Shipping Companies

<Figure 1> Factors and attributes of the EMSMM

1. Security Culture	2. Management and Employee Commitment	3. Security Assessment	4. Security Policy, System and Procedures	5. Documentation and Communication	6. Process Control	7. Continuous Security Improvement	8. Security Incidents Handling and Continuity of Operations	9. Business Partners Security
<p>A1.1. Senior management promotes security as an essential part of every day organizational activity.</p> <p>A1.2. Security issues are included in the agendas of scheduled management meetings.</p> <p>A1.3. Training seminars and courses on maritime security are conducted for managers.</p> <p>A1.4. Security trainings, exercises and seminars are periodically conducted for employees.</p> <p>A1.5. Security information is periodically distributed among employees by email, posters, videos, etc.</p>	<p>A2.1. Security related roles and responsibilities are clearly identified and documented for employees.</p> <p>A2.2. The procedures for security related decision making are clearly identified and documented.</p> <p>A2.3. Senior management considers security investments as a service quality improvement facilitator.</p> <p>A2.4. Senior management allocates adequate resources for security improvement.</p> <p>A2.5. Employees from different levels are involved in processes of security related decision making.</p> <p>A2.6. Procedures for employees to report security errors and breaches are established.</p> <p>A2.7. A platform for employees to propose necessary changes and possible solutions is established.</p> <p>A2.8. Reward & Recognition program is established to motivate employees to provide security feedback.</p>	<p>A3.1. The internal security audit of all activities and departments is periodically conducted.</p> <p>A3.2. Security related risks are periodically identified.</p> <p>A3.3. Security risk assessment is conducted to derive a risk magnitude.</p> <p>A3.4. Risk acceptance levels are established based on risk magnitudes and existing control barriers.</p> <p>A3.5. Measures are implemented to mitigate identified risks according to risk acceptance levels.</p> <p>A3.6. Investments in security are made according to risk magnitude and risk acceptance levels.</p> <p>A3.7. All prospective employees periodically go through background screening for security purposes.</p> <p>A3.8. A background screening of all current employees is periodically conducted for security purposes.</p>	<p>A4.1. A well-structured security management policy is developed and documented.</p> <p>A4.2. Security management policy includes security management system, procedures, plans, etc.</p> <p>A4.3. Security policy is included into overall company policy.</p> <p>A4.4. Security policy, system, procedures, plans do not contradict with other measures and procedures.</p> <p>A4.5. Security measures are integrated into daily activities.</p>	<p>A5.1. A communication system is established with authorities, partners, agents for security purposes.</p> <p>A5.2. Detailed procedures for security communication are developed and documented.</p> <p>A5.3. Data and processes in the communication system are periodically backed up.</p> <p>A5.4. Measures to secure communication and information are developed and implemented.</p> <p>A5.5. Documentation and information systems are periodically backed up.</p> <p>A5.6. IT security measures are implemented.</p>	<p>A6.1. Management promotes the idea of security prevention by making it right from the first time.</p> <p>A6.2. A measurement system is developed and put in place to monitor and review all security processes.</p> <p>A6.3. A proofreading system is used to detect security loopholes and implement corrections immediately.</p> <p>A6.4. Tracking and tracing technologies are implemented for commercial and security purposes.</p> <p>A6.5. Procedures for detection and response to security incidents are clearly defined and documented.</p> <p>A6.6. Investments in technologies, software and/or equipment are made to improve access control.</p>	<p>A7.1. Security procedures are constantly reviewed and improved according to security requirements.</p> <p>A7.2. Security targets, methods and a time line are clearly established and documented.</p> <p>A7.3. Corrective actions and removal of the root cause of security errors are timely undertaken.</p> <p>A7.4. We conduct research on security improvement and/or participate in similar projects.</p>	<p>A8.1. We consider and predict all various scenarios of maritime security threats.</p> <p>A8.2. Disaster, crisis management and emergency plans are developed based on considered scenarios.</p> <p>A8.3. Training and drills on disaster and crisis management are periodically conducted.</p> <p>A8.4. Recovery and business continuity plans are developed and reviewed.</p> <p>A8.5. Training and drills on recovery and business continuity management are periodically conducted.</p> <p>A8.6. Dedicated communication channels exist for emergency cases.</p>	<p>A9.1. All future business partners undergo security background checks.</p> <p>A9.2. All current partners are periodically assessed to ensure their compliance with security requirements.</p> <p>A9.3. Security trainings and exercises are jointly organized with business partners.</p> <p>A9.4. Collaboration with business partners exists to identify, mitigate and share security risks.</p> <p>A9.5. Liabilities for possible security incidents are clearly defined in contracts with business partners.</p>

Source: Sadovaya and Thai (2014)

<Figure 2> Organizational performance of shipping companies

1. Security Performance	2. Business Resilience	3. Other Business Performance
<p>B1.1. Number of cargo pilferage</p> <p>B1.2. Number of stowaways</p> <p>B1.3. Number of ship attacks, including terrorist and piracy attack, armed robbery</p> <p>B1.4. Number of tampering with cargo, data and physical shipmen</p> <p>B1.5. Cargo loss and damage</p> <p>B1.6. Number of smuggling</p> <p>B1.7. Number of violations of security rules by employees</p> <p>B1.8. Number of prevented security incidents</p> <p>B1.9. Level of employees' knowledge on security requirements, measures, threats, risks.</p>	<p>B2.1. Time taken to identify security problems</p> <p>B2.2. Time taken to mitigate security problems</p> <p>B2.3. Time taken to recover from security incidents</p> <p>B2.4. Customer service level during disruption compared to normal operation time</p>	<p>B3.1. Total cost per TEU or per ton</p> <p>B3.2. Profit margin per TEU or per ton</p> <p>B3.3. Level of competitiveness</p> <p>B3.4. Level of reputation for liability</p> <p>B3.5. Level of market share</p> <p>B3.6. Vessels' port turnaround time</p> <p>B3.7. Vessels' total voyage time</p> <p>B3.8. Vessels' schedule delays because of security issues</p> <p>B3.9. Number of Port State Control inspections on your company's vessels</p> <p>B3.10. Additional cost because of security issues</p> <p>B3.11. Level of business process's interruptions</p> <p>B3.12. Level of use of track and trace system</p> <p>B3.13. Level of on-time delivery of cargo</p> <p>B3.14. Level of documentation accuracy</p> <p>B3.15. Level of flexibility in responding to customer requests</p> <p>B3.16. Level of customers' overall satisfaction about physical resources</p> <p>B3.17. Level of customers' overall satisfaction about quality of service provided</p> <p>B3.18. Number of new customers</p> <p>B3.19. Number of repeated customers</p>

The test for non-response bias was conducted to compare responses received after the first mail-out and those collected after each of reminder letters. The results of ANOVA test, at the 5% significance level, showed no significant difference between groups of responses. Based on the business sector characteristics, the respondents' companies are distributed as follows: 23% represent both shipping and ship management companies, 23% are shipping companies, 43% represent ship management companies, and 6% of respondents were from other types of companies, such as logistics, consultancy, brokering, offshore supply and others, whereas 5% of respondents did not indicate their company type.

IV. Analysis and Results

1. The EMSMM

To validate the structure of the EMSMM, it was first analyzed through the EFA, based on the principle components methods and Varimax rotation technique. During several runs of the EFA, 22 items were dropped one by one, using the commonly accepted procedure, where the item should be withdrawn if it is not loaded highly enough on one factor (i.e. more than 0.5) or highly loaded on several factors (Thai, 2013). The analysis on the remaining 31 items resulted in six factors explaining 72.447% of variances, where Factor 1 explains 42.127% of variances, Factor 2 explains 11.477%, 5.608% explained by Factor 3, 5.191% by Factor 4, 4.15% by Factor 5, and 3.894% by Factor 6 respectively. The value of the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy (0.884), greater than required 0.60, and the value of Barlett's test of sphericity ($p = 0.000$) confirms a good strength of inter-correlations of the last run of the EFA (Hair et al., 2010).

To further validate the model, the CFA was then performed. The CFA was run several times to derive a model with the best model fit characteristics. During the analysis, items loaded lower than 0.70 to its factor were eliminated. Overall, nine more items were withdrawn. The decision to drop an item was also based on its significance for the meaning of its corresponding factor. For example, the factor of "COMIT" has only two items left as a result of the CFA, however these items fully represent

the meaning of the factor. As shown in Figure 3, the model resulted from the CFA contains 22 measurable items and has the model fit characteristics satisfying the suggested standards (Hair et al., 2010). Thus, for a good model fit, the recommended minimum discrepancy/degree of freedom (CMIN/DF) is smaller than 3.0 (good level), comparative fit index (CFI) is greater than 0.90 (good level), root mean square error of approximation (RMSEA) is less than 0.05 (good level) or less than 0.10 (moderate level), root mean square residual (RMR) is less than 0.05 (Blunch, 2013). The model resulted from the last run of CFA has the following model fit characteristics and, therefore, supports the results of the EFA: CMIN/DF = 1.934, RMR = 0.037, CFI = 0.918, GFI = 0.808, NFI = 0.846, and RMSEA = 0.085. The model was also tested for reliability and validity (Hair et al., 2010; Blunch, 2013). The results shown in Table 4 indicate that the model satisfies the requirements and therefore has no reliability and validity issues.

Based on the changes in the model resulting from the analysis and validation, the sub-hypotheses in this study were specified as shown in Figure 4.

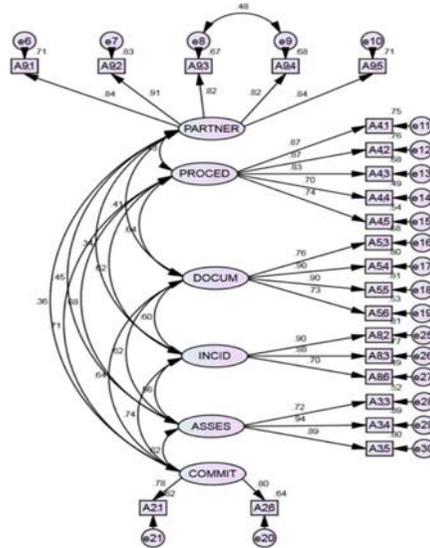
2. Organizational Performance

To test the relationship between the model's factors and organizational performance of shipping companies, the categories were first validated through the EFA. After dropping eight items the analysis revealed a good strength of inter-correlations ($KMO = 0.758$, $p = 0.000$). As a result of the last run, six factors explain 71.156% of variances were extracted, including Factor 1 (22.580%), Factor 2 (19.419%), Factor 3 (10.951%), Factor 4 (6.970%), Factor 5 (6.533%), and Factor 6 (4.702%). Names of Factors 1 and 2 were kept the same, Security Performance (SECURITY) and Business Resilience (RESILIENCE) respectively. The measurement items of the initial category of other business performance are distributed into four factors: Market Performance (MARKET) with items B3.2, B3.3 B3.4, Time Performance (TIME) containing items B3.6 and B3.7, Security Related Performance (SECRELAT), consisting of items B3.8, B3.9, B3.10, and Customer Performance (CUSTOMER) with items B3.14, B3.15, B3.16, B3.17, B3.18 and B3.19.

<Table 4> Results of the validity and reliability test in CFA

Factors	CR	AVE	MSV	ASV	Cronbach's Alpha
INCID	.869	.691	.554	.346	.844
PARTNER	.927	.719	.202	.160	.930
PROCED	.900	.644	.511	.390	.893
DOCUM	.894	.680	.410	.346	.883
COMMIT	.770	.627	.554	.398	.783
ASSES	.891	.733	.462	.352	.867
Required:	> 0.7; > AVE	> 0.5	< AVE	< AVE	> 0.6

<Figure 3> Factors of the EMSMM resulted from the CFA



<Figure 4> Sub-hypotheses of the study

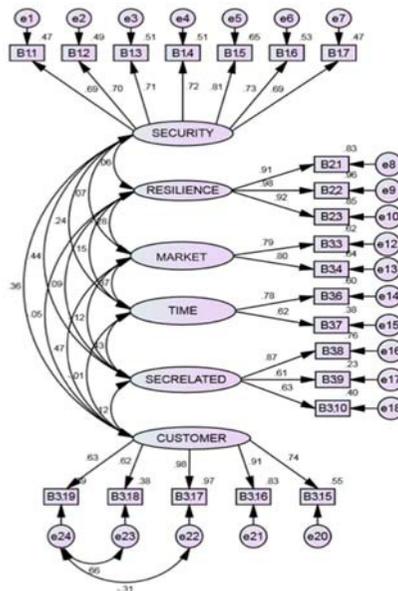
Hypothesis 1	H1.1. Management and Employee Commitment positively impacts security performance. H1.2. Security Assessment positively impacts security performance. H1.3. Developed and implemented Security Policy, System and Procedures positively impact security performance. H1.4. Documentation and Communication Security positively impacts security performance. H1.5. Measures for Security Incidents Handling and Continuity of Operations positively impact security performance. H1.6. Business Partners Security positively impacts security performance.
Hypothesis 2	H2.1. Management and Employee Commitment positively impacts business resilience. H2.2. Security Assessment positively impacts business resilience. H2.3. Developed and implemented Security Policy, System and Procedures positively impact business resilience. H2.4. Documentation and Communication Security positively impacts business resilience. H2.5. Measures for Security Incidents Handling and Continuity of Operations positively impact business resilience. H2.6. Business Partners Security positively impacts business resilience.
Hypothesis 3	H3.1. Management and Employee Commitment positively impacts other business performance. H3.2. Security Assessment positively impacts other business performance. H3.3. Developed and implemented Security Policy, System and Procedures positively impact other business performance. H3.4. Documentation and Communication Security positively impacts other business performance. H3.5. Measures for Security Incidents Handling and Continuity of Operations positively impact other business performance. H3.6. Business Partners Security positively impacts other business performance.

To further validate the structure of organizational performance, the CFA was run several times to achieve the best model-fit characteristics. To improve validity and reliability of the measurement model, items B3.2 and B3.14 were withdrawn based on their low loadings. Besides, their dropping did not change the semantic meaning of the factors they belong to. The last run of CFA of organizational performance resulted in the following model fit characteristics: CMIN/DF = 1.310; RMR = 0.048; CFI = 0.954; GFI = 0.821; RMSEA = 0.055. Therefore, the six factors of organizational performance and 22 measurement items, as shown in Figure 5, contribute to a good model fit and support the results of the EFA. The model was then examined for the validity and reliability concerns. As Table 5 shows, the model is considered as valid and reliable.

<Table 5> Validity concern check for the categories of organizational performance

<i>Categories</i>	<i>CR</i>	<i>AVE</i>	<i>MSV</i>	<i>ASV</i>	<i>Cronbach's Alpha</i>
SECRETAT	.776	.541	.197	.084	.691
SECURITY	.883	.519	.197	.079	.881
RESILIENCE	.956	.878	.080	.023	.955
MARKET	.772	.629	.225	.092	.771
TIME	.718	.560	.188	.081	.648
Required:	> 0.7;	> AVE > 0.5	< AVE	< AVE	> 0.6

<Figure 5> Categories of organizational performance resulted from the CFA



3. A Link between the EMSMM and Organizational Performance

Based on the empirical analyses conducted earlier, the structural model was constructed, whereas six factors of the EMSMM and six categories of organizational performance represent independent and dependent variables respectively. The structural model is aimed to test the relationship between the EMSMM and organizational performance of shipping companies. Specifically, the relationships between each model's factor and six categories of organizational performance are measured.

Because the single survey was used to collect data for both dependent and independent variables, it is recommended to test for common method bias (Lowry et al., 2013). For this purpose, the unmeasured common latent factor (CLF) was added to the measurement model to retrieve the common variance. The CLF includes all dependent and independent variables from all other latent factors. The items loadings on the CLF are constrained to be equal to ensure the unstandardized loadings are equal. Squaring the unstandardized loading then gives the value of the common method bias. The effect of the common method bias can be controlled by retaining the CLF in the consequent measurement model. The result showed that some of the variables of Documentation and Communication factor can be due to common method bias. To control the bias the CLF was retained in the model. The data were then imputed from AMOS to SPSS. The imputed data were used to create a structural model with independent and dependent observed variables in SEM. The measurement model was also tested for reliability and validity issues. The results shown in Table 6 confirm the absence of validity and reliability concerns.

The first run of the SEM showed that some paths between variables were not significant. It was also observed that significant relationships exist between some dependent variables. Thus, to improve the model fit characteristics, some paths were deleted and some variables were used as mediator variables. The final version after conducting the SEM is shown in Figure 6. Table 7 shows results of hypothesis testing. The hypothesized relationships were tested using the associated standardized regression coefficient of the paths. It can be seen that PROCED has a significant positive impact on SECURITY ($\beta=0.385$), therefore H1.3 is supported. There are also positive relationships existing between PARTNER and SECURITY, and COMMIT and SECURITY ($\beta=0.151$ and $\beta=0.166$

respectively), hence H1.6 and H2.1 are also supported. The link between COMMIT and TIME ($\beta=0.915$) is also significant, implying the partial support of H3.1. The hypothesis is supported partially, since only one among four categories of Other Organizational Performance is positively impacted. Similarly, H3.3, H3.4 and H3.6 are supported partially, since only one category among four is impacted positively. Specifically, PROCED has a positive link on CUSTOMER ($\beta=0.269$), DOCUM positively impacts TIME ($\beta=0.516$), and the relationship between PARTNER and CUSTOMER are also positive ($\beta=0.220$). H3.2 is rejected, because the significant negative relationship between ASSES and TIME was found ($\beta=-0.238$). Similarly, negative impact of INCID on TIME implies the rejection of H3.5 ($\beta=-0.578$).

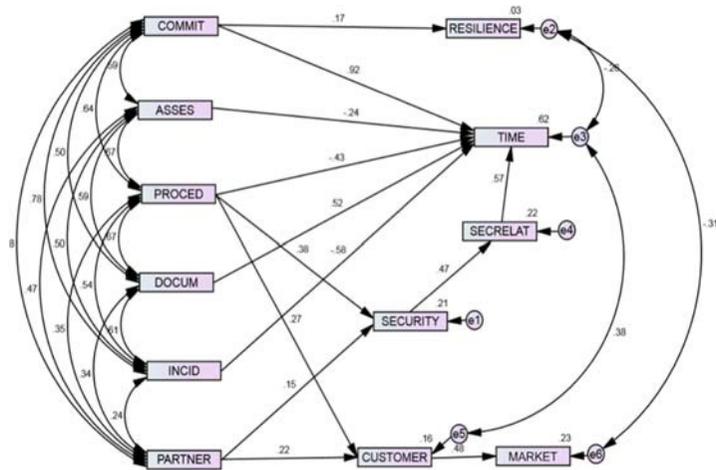
<Table 6> Results of the validity and reliability test

<i>Variables</i>	<i>CR</i>	<i>AVE</i>	<i>MSV</i>	<i>ASV</i>	<i>Cronbach's Alpha</i>	
COMMIT	.787	.649	.563	.190	.783	
SECURITY	.883	.520	.192	.085	.881	
RESILIENCE	.956	.879	.078	.015	.955	
MARKET	.772	.629	.228	.053	.771	
TIME	.721	.565	.184	.040	.648	
SECRELAT	.776	.542	.192	.060	.691	
CUSTOMER	.885	.616	.228	.078	.897	
PROCED	.902	.650	.483	.208	.893	
PARTNER	.926	.715	.247	.115	.930	
INCID	.850	.658	.563	.172	.844	
DOCUM	.891	.673	.483	.197	.883	
ASSES	.883	.719	.413	.172	.867	
Required:	> 0.7;	> AVE	> 0.5	< AVE	< AVE	> 0.6

<Table 7> Relationship testing between the EMSMM and organizational performance

	<i>Paths</i>	<i>Hypotheses</i>	<i>Standardized path coefficients</i>	<i>Results</i>
SECURITY	<--- PROCED	H1.3	0.385	Supported
SECURITY	<--- PARTNER	H1.6	0.151	Supported
RESILIENCE	<--- COMMIT	H2.1	0.166	Supported
TIME	<--- COMMIT	H3.1	0.915	Supported
TIME	<--- ASSES	H3.2	-0.238	Not supported
TIME	<--- PROCED	H3.3	-0.434	Not supported
CUSTOMER	<--- PROCED		0.269	
TIME	<--- DOCUM	H3.4	0.516	Supported
TIME	<--- INCID	H3.5	-0.578	Not supported
CUSTOMER	<--- PARTNER	H3.6	0.220	Supported

<Figure 6> Results of the SEM with six independent and six dependent variables



Notes: Model fit statistics: CMIN = 64.361; DF = 34; CMIN/DF = 1.893; CFI = 0.951; GFI = 0.918; AGFI = 0.811; NFI = 0.906; RMSEA = 0.093; and PCLOSE = 0.027; All coefficients are standardized.

V. Findings and Discussion

In this study we aimed to examine the relationship between the proposed EMSMM and organizational performance of shipping companies. Through the literature review and further statistical analysis the model was validated and resulted in six factors and 22 attributes. Besides, as a result of the EFA and CFA, three initially proposed categories of organizational performance were divided into six, namely Security Performance, Business Resilience, Market Performance, Time Performance, Security Related Performance, and Customer Performance.

The relationship between the model's factors and each category of organizational performance were then studied. It was found that the category of Security Performance is positively affected by factors of Security Policy, System and Procedures and Business Partners Security, and leads to a positive impact on Security Related and Time Performance. Besides, the category of Customer Performance, which has a positive relationship with Market Performance, is positively affected by factors of Security Policy, System and Procedures and Business Partners Security. The category of Business Resilience is found to be positively impacted by the factor of Management and Employee Commitment. Moreover, this

factors together with the factor of Documentation and Communication showed positive impacts on the category of Time Performance. However, it was also found that the category of Time Performance is negatively influenced by some model's factors, such as Security Policy, System and Procedures, Security Incidents Handling and Continuity of Operations, and Security Assessment. These negative relationships were expected, since the literature review showed negative impacts on performance related to time. However, it is believed that the time performance should be improved when the effective security management becomes an integrated part of daily activities. Besides, these negative relationships they do not compromise the validity of the factors.

The results of the statistical analyses provide a solid foundation for an effective MSM in shipping companies. Shipping companies are recommended to conduct periodical assessment of their organizational performance using the proposed categorization. Based on this assessment necessary changes should be implemented according to corresponding factors of the EMSMM.

VI. Conclusion

By studying the impacts of the proposed EMSMM for shipping companies on their organizational performance, this paper contributes to the understanding of how security can be managed effectively. For the purpose of the study, the information on security management practices, as well as on changes in organizational performance was collected from shipping companies all over the world. The collected data were analyzed using the EFA, CFA and SEM. The results showed positive relationships between the model and organizational performance. The categories of Security Performance and Customer Performance are positively affected by factors of Security Policy, System and Procedures and Business Partners Security. Therefore, shipping companies are recommended to pay a special attention to these areas of security management.

This paper has both academic and managerial implications. First, it provides a valuable contribution to the literature on organizational performance of shipping companies by introducing categories and indicators of performance that can be applicable for measuring impacts of security management. This categorization is recommended for using by

shipping companies to measure an effectiveness of their security management and implemented security requirements.

Besides, the paper represents one of the first studies conducted on the impacts of effective security management in shipping companies on their organizational performance. It not only shows the effectiveness of the proposed model but also describes the relationship between its factors and categories of organizational performance. The understanding of these relationships can help shipping companies to improve their MSM by using the proposed categorization and the EMSMM together.

This study has several limitations. First, it might be argued that the number of responses may jeopardize the results' accuracy. However, it can be seen that the number was enough to analyze the data by using all three methods. Besides, the impacts on the Business Resilience category were not clearly identified. One of the reasons is the lack of information on security accidents, where resilience can be jeopardized. Thus, further research is recommended to study a relationship between the EMSMM and Business Resilience. For this purpose, the sample population should be constructed from companies with records of major security accidents.*

* Date of Contribution; October 30, 2014
Date of Acceptance; May 1, 2015

References

- BICHOU, K. (2008), "Security and risk-based models in shipping and ports: Review and critical analysis", Paper presented at the OECD/ITF Round Table on Security, Risk Perception and Cost-Benefit Analysis, 11-12 December, Paris, France.
- BICHOU, K., SZYLLOWICZ, J. S. and ZAMPARINI, L. (2014), *Maritime Transport Security: Issues, Challenges and National Policies*, Edward Elgar Publishing, U.K., U.S.A.
- BLUNCH, N. J. (2013), *Introduction to Structural Equation Modeling Using IBM SPSS Statistics and AMOS*, 2nd ed., SAGE.
- BRYANT, D. L. (2009), "The outlook for maritime security", *Journal of Commerce*, 12 January, p. 56.
- CLOSS, D., SPEIER, C., WHIPPLE, J. and VOSS, M. D. (2008), "A framework for protecting your supply chain", *Supply Chain Management Review*, Vol. 12, No. 2, pp. 38-45.
- CRUTCH, M. (2006), "The benefits of investing in global supply chain security: Executive summary from the CVCR 2006 roundtable meeting", Center for Value Chain Research, Lehigh University, U.S.
- EVANS, J. R. (2007), "Impacts of information management on business performance", *Benchmarking: An International Journal*, Vol. 14, No. 4, pp. 517-533.
- FENG, M., TERZIOVSKI, M. and SAMSON, D. (2008), "Relationship of ISO 9001:2000 quality system certification with operational and business performance. A survey in Australia and New Zealand-based manufacturing and service companies", *Journal of Manufacturing Technology Management*, Vol. 19, No. 1, pp. 22-37.
- GONZÁLEZ-BENITO, J. (2007), "A theory of purchasing contribution to business performance", *Journal of Operations Management*, Vol. 25, No. 4, pp. 901-917.
- GOULD, J., MACHARIS, C. and HAASIS, H. (2010), "Emergence of security in supply chain management literature", *Journal of Transportation Security*, Vol. 3, No. 4, pp. 287-302.
- GOULIELMOSA, A. M., ANASTASAKOSB, A. and GATZOLI, A. (2014), "The Effect of Maritime Security Regime (ISPS Code), on World Supply of Seafarers", *SPOUDAI Journal of Economics and Business*, Vol. 64, No. 1, pp. 63-77.
- GREEN, K. W., WHITTEN, D. and INMAN, R. A. (2008), "The impact of logistics performance on organizational performance in a supply chain context", *Supply Chain Management: An International Journal*, Vol. 13, No. 4, pp. 317-327.

GUTIÉRREZ, X. (2007), “A Model for the Design of Effective and Resilient Supply Chain Security Management Systems”, Ph.D. thesis, Ecole polytechnique fédérale de Lausanne, Switzerland.

GUTIÉRREZ, X., HINTSA, J., WIESER, P. and HAMERI, A. P. (2007), “Voluntary supply chain security program impacts: an empirical study with BASC member companies”, *World Customs Journal*, Vol. 1 No. 2, pp. 31-48.

HAIR, J., BLACK, W., BABIN, B. and ANDERSON, R. (2010), *Multivariate Data Analysis*, 7th ed., Pearson Prentice Hall, Upper Saddle River, New Jersey.

HINTSA, J., GUTIERREZ, X., WIESER, P. and HAMERI, A. P. (2009), “Supply Chain Security Management: An overview”, *International Journal of Logistics Systems and Management*, Vol. 5, No. 3, pp. 344-355.

LOWRY, P. B., GASKIN, J., TWYMAN, N., HAMMER, B. and ROBERTS, T. L. (2013), “Taking “Fun and Games” Seriously: Proposing the Hedonic-Motivation System Adoption Model (HMSAM)”, *Journal of the Association for Information Systems*, Vol. 14, No. 11, pp. 617-671.

MACDONALD, J. R. and CORSI, T. M. (2013), “Supply Chain Disruption Management: Severe Events, Recovery, and Performance”, *Journal of Business Logistics*, Vol. 34, No. 4, pp. 270–288.

SADOVAYA, E. and THAI, V. V. (2014), The Effective Maritime Security Management Model (EMSMM): A perspective from practitioners in Singapore. *Security Journal advance online publication*, 10 March 2014; doi:10.1057/sj.2014.13.

THAI, V. V. and GREWAL, D. (2007), “The maritime security management system: Perceptions of the international shipping community”, *Maritime Economics and Logistics*, Vol. 9, No. 2, pp. 119-137.

THAI, V. V. (2007), “Impacts of security improvements on service quality in maritime transport: An empirical study of Vietnam”, *Maritime Economics and Logistics*, Vol. 9, No. 4, pp. 335-356.

THAI, V. V. (2009), “Effective maritime security: conceptual model and empirical evidence”, *Maritime Policy and Management: The Flagship Journal of International Shipping and Port Research*, Vol. 36, No. 2, pp. 147-163.

THAI, V. V. (2013), “Logistics service quality: Conceptual model and empirical evidence”, *International Journal of Logistics: Research and Applications*, Vol. 16, No. 2, pp. 114–131.

TIMLEN, T. (2007), “The ISPS Code: Where are we now?” *Cargo Security International*, April/May, pp. 14-15.

URCIUOLI, L., STERNBERG, H. and EKWALL, D. (2010), "The effects of security on transport performances", Paper presented at the 12th World Conference on Transport Research, 11-15 July, Lisbon, Portugal.

VOSS, M., WHIPPLE, J. and CLOSS, D. (2009), "The role of strategic security: Internal and external security measures with security performance implications", *Transportation Journal*, Vol. 48, No. 2, pp. 5-23.

WILLIAMS, Z. (2008), "Supply chain security: An institutional approach to strategies and outcomes", Ph.D. thesis, Mississippi State University, Mississippi, United States.

YANG, Y. C. (2010), "Impact of the container security initiative on Taiwan's shipping industry", *Maritime Policy and Management*, Vol. 37, No. 7, pp. 699-722.