Effective management of maritime security in shipping companies

Sadovaya, Elena

2015

Sadovaya, E. (2015). Effective management of maritime security in shipping companies.
Doctoral thesis, Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/65351>

<https://doi.org/10.32657/10356/65351>

EFFECTIVE MANAGEMENT OF MARITIME SECURITY IN SHIPPING COMPANIES

ELENA SADOVAYA
SCHOOL OF CIVIL AND ENVIRONMENTAL ENGINEERING
2015

EFFECTIVE MANAGEMENT OF MARITIME SECURITY IN SHIPPING COMPANIES

ELENA SADOVAYA

School of Civil and Environmental Engineering

A thesis submitted to the Nanyang Technological University
in fulfilment of the requirements for the degree of
Doctor of Philosophy

2015

SUMMARY

During the last ten years, maritime security has become an important issue on the international maritime agenda. The diversity of security requirements brings a problem of effective security management in shipping companies and may impact their organizational performances significantly. Therefore, this research project aims to develop and validate an Effective Maritime Security Management Model (EMSMM) for shipping companies and to study its impacts on their organizational performance. It addresses three main research questions, focusing on maritime security regulations and requirements, effective maritime security management, and its impacts on organizational performance. A comprehensive literature review was conducted to study existing maritime security regulations and management approaches as well as earlier proposed models and systems applicable for security management to derive a detailed list of compulsory and voluntary security requirements imposed on shipping companies and essential criteria for the EMSMM. Besides, the literature on reported and proposed impacts of security management on organizational performance of shipping companies was analyzed and the list of impacts was composed. Based on the reviewed literature, the EMSMM was developed.

To empirically validate the model, thirteen in-depth interviews, one main survey and one confirmatory survey were conducted. The sampling population was constructed from industry practitioners responsible for security management in shipping companies worldwide. To analyse the collected information, thematic and statistical methods as well as the analytical hierarchy process (AHP) technique were applied in this study. Statistical methods, such as the exploratory and confirmatory factor analyses (EFA and CFA) and the structural equation modelling (SEM), were used to validate the EMSMM and to analyse its impacts on the organizational performance of the participating companies. Further, to rank the importance of the model's factors, the AHP technique was applied. The results confirmed that the EMSMM consists of six factor, namely, Management and Employee Commitment, Security Policy, System and Procedures, Security Assessment, Security Incidents Handling and Continuity of Operations, Business Partners Security, and

Documentation and Communication. The impacts of security management on organizational performance were measured according to three categories of performance, namely, Security Performance, Business Resilience and Other Organizational Performance, where the last category was further divided into Security Related, Time, Customer and Market Performance. The results of this project confirmed the overall positive impact of the proposed EMSMM on the organizational performance of shipping companies. However, it is important for managers to implement all factors together in order to achieve these positive results. Apart from enriching the literature on maritime security management, the proposed model can be used as a security management toolbox which can help senior management in shipping companies to manage security effectively. However, further research is needed to study the relationship between the EMSMM and Business Resilience, since this relationship is not significant due to the shortage of data on actual security accidents.

DEDICATION

This thesis is dedicated to my mother, Dr. Malyugina Tatyana, who continues to learn, grow and develop and who has been a source of encouragement and inspiration to me throughout my life.

ACKNOWLEDGMENT

Firstly, I would like to express my sincere gratitude to my supervisor Assistant Professor Thai Van Vinh, who believed in my abilities and invited me to become his student. I learned so much from our discussions and I appreciate his patience and valuable advice.

Sincere thanks go to the professors from Nanyang Technological University (NTU) and other universities for their valuable advice, as well as industry professionals who provided me with practical suggestions.

I am very grateful to all interviewees and survey respondents who helped me with this research. Without their kind support, this research would not have been possible.

Besides, I would like to express my sincere thanks to the ICC International Maritime Bureau for sharing the data on accidents of piracy and armed robbery against ships.

I would also like to thank my friends and classmates Ms Tan Shi Yun Beverly Ms Loh Hui Shan, Mr Yuen Kum Fai and Ms Zhang Guizhen for their warm friendship and constant support and help from the first day of my study in NTU.

Last but not least, I am thankful to my family and friends for their support and understanding.

TABLE OF CONTENTS

SUMMARY	i
DEDICATION	iii
ACKNOWLEDGMENTS	iv
TABLE OF CONTENTS	v
LIST OF TABLES	ix
LIST OF FIGURES	xi
LIST OF ABBREVIATIONS	xii
CHAPTER 1. INTRODUCTION	1
1.1. Scope	1
1.2. Background Information	1
1.3. Research Problems, Aims, Questions and Objectives	6
1.4. Research Methods	9
1.5. Structure of the Thesis	10
CHAPTER 2. LITERATURE REVIEW	12
2.1. Introduction	12
2.2. Maritime Security Regulations and Requirements for Shipping Companies	12
2.2.1. Maritime Security Regulations	13
2.2.2. Maritime Security Requirements	16
2.2.2.1. Classification of Maritime Security Requirements	16
2.2.2.2. Current Issues with Existing Maritime Security Requirements .	32
2.2.2.3. Implementation of Maritime Security Requirements	36
2.3. Effective Maritime Security Management in Shipping Companies	36
2.3.1. Definition of Maritime Security Management	37
2.3.2. Existing Approaches and Models of Maritime Security Management	38
2.3.3. Problems of Maritime Security Management in Shipping Companies	45
2.3.4. Essential Criteria for the EMSMM in Shipping Companies	47
2.4. The Link between Maritime Security and Organizational Performance of Shipping Companies	52

2.4.1. Impacts of Implementation of Maritime Security Requirements	52
2.4.2. Organizational Performance of Shipping Companies	61
2.4.3. Measurement of Impacts of Maritime Security Management on Organizational Performance of Shipping Companies	66
2.5. Summary of Literature Review	70
CHAPTER 3. METHODOLOGY	74
3.1. Introduction	74
3.2. Research Questions	74
3.3. Research Approach	75
3.4. Research Process	76
3.5. Model Building and Hypotheses Development	81
3.6. Data Collection	101
3.6.1. Exploratory Interviews	101
3.6.1.1. Population and Sampling	101
3.6.1.2. Interview Form and Procedure	103
3.6.2. Main Survey	104
3.6.2.1. Population and Sampling	104
3.6.2.2. Design of the Questionnaire	106
3.6.2.3. Questionnaire Pretesting	106
3.6.2.4. Survey Administration	110
3.6.2.5. Response Rate	112
3.6.2.6. Data Editing, Coding, Categorising and Entry Process	113
3.6.3. AHP Survey	114
3.6.3.1. Population and Sampling	115
3.6.3.2. Design of the AHP Questionnaire	116
3.6.3.3. Survey Administration	117
3.6.3.4. Data Editing, Coding, Categorising and Entry Process	117
3.7. Errors and the Ways Used to Reduce Them	117
3.8. Methods of data analysis	118
3.9. Summary	119
CHAPTER 4. EFFECTIVE MARITIME SECURITY MANAGEMENT IN SHIPPING COMPANIES	120

4.1. Introduction	120
4.2. Statistical Techniques for Data Analysis	120
4.3. Respondents Profile	125
4.4. Perception of the EMSMM in Shipping Companies	129
4.4.1. General View of Maritime Security Management (MSM) in Shipping Companies	129
4.4.2. The Implementation of Security Requirements in Shipping Companies	131
4.4.3. Validation of the EMSMM	132
4.5. Measurement Validity and Reliability Analysis	140
4.6. Perception of the EMSMM's Factors based on the Respondents' Designation and Trading Areas of Their Companies	143
4.7. Relative Importance of the Factors of the EMSMM: Perception of Nine Experts	145
4.8. Discussion	148
4.9. Summary	152
CHAPTER 5. IMPACTS OF MARITIME SECURITY MANAGEMENT ON ORGANIZATIONAL PERFORMANCE OF SHIPPING COMPANIES	155
5.1. Introduction	155
5.2. Statistical Techniques for Data Analysis	155
5.3. Relationship between Implementation of the EMSMM and Organizational Performance	157
5.3.1. Categories of Organizational Performance	157
5.3.2. Common Method Bias	163
5.3.3. Construct Reliability and Validity	164
5.3.4. Hypothesis Testing	165
5.4. Discussion	174
5.5. Summary	180
CHAPTER 6. DISCUSSIONS AND CONCLUSIONS	182
6.1. Introduction	182
6.2. Discussion of the Findings	182
6.3. Implication	189

6.3.1. Academic Implication	189
6.3.2. Managerial and Regulatory Implication	192
6.3.2.1. Recommendations to Shipping and Ship Management Companies on Effective Management of Maritime Security	194
6.4. Research Limitations	198
6.5. Future Research	200
REFERENCES	202
APPENDICES	221
APPENDIX 1. IN-DEPTH INTERVIEWS	221
Appendix 1.1. Cover Letter	221
Appendix 1.2. Interview Information Sheet	222
Appendix 1.3. Sample of Interview Form	224
APPENDIX 2. MAIN SURVEY	228
Appendix 2.1. Sample of Questionnaire Pre-test Form	228
Appendix 2.2. Cover Letter	229
Appendix 2.3. Reminder Letter	230
Appendix 2.4. Samples of Questionnaire	231
Appendix 2.4.1. Questionnaire in Word document	231
Appendix 2.4.2. Online Questionnaire	236
APPENDIX 3. CONFIRMATORY SURVEY	242
Appendix 3.1. Cover Letter	242
Appendix 3.2. Sample of Questionnaire	243
Appendix 3.3. Matrix Resulted from the Questionnaire	248
Appendix 3.4. Results of the Confirmatory (AHP) Survey	249
APPENDIX 4. NON-RESPONSE BIAS TEST	250

LIST OF TABLES

Table 1.1	List of ships hijacked by LTTE from 1995 till 2009	5
Table 1.2	Research aims, questions and objectives	8
Table 2.1	Maritime security regulations for shipping companies	16
Table 2.2	Maritime security requirements for shipping companies	28
Table 2.3	Compulsory and voluntary maritime security requirements for shipping companies	35
Table 2.4	Management approaches of security management in existing literature	43
Table 2.5	Essential criteria for the EMSMM in shipping companies	51
Table 2.6	BASC Certification and maintenance average cost for different turnovers	56
Table 2.7	Impacts of implementation of maritime security requirements on organizational performance of shipping companies	57
Table 2.8	Summary of the impacts of implementation of security requirements on organizational performance of shipping companies.	59
Table 2.9	Definitions of organizational performance given by different authors	61
Table 2.10	Categories of organizational performance found in the literature..	65
Table 2.11	Gaps of the reviewed literature and solutions	73
Table 3.1	Summary of research stages and results according to aims	80
Table 3.2	Management approaches and essential criteria used to develop nine factors of the EMSMM	89
Table 3.3	Literature sources, components of the factors and associated attributes	90
Table 3.4	Interviewees' designation	102
Table 3.5	Interviewees' experience in the security related job or industry...	103
Table 3.6	Types of vessels owned or operated by the companies of the interviewees	103
Table 3.7	Percentage and number of the companies in the mailing list according to the world's regions	105
Table 3.8	Number of factors and attributes after each step of model	

	development	107
Table 3.9	Factors and attributes of the EMSMM	108
Table 3.10	Categories of organizational performance of shipping companies and their indicators	110
Table 3.11	Scale of relative importance	116
Table 4.1	KMO and Bartlett's Test – last run of factor analysis	133
Table 4.2	EFA with Varimax rotation results	135
Table 4.3	Perceptions of the attributes of the EMSMM's factors	138
Table 4.4	Perceptions of the factors of the EMSMM	139
Table 4.5	Profile of the interviewed companies with regard to implementation and importance of the model's factors	140
Table 4.6	Results of the validity and reliability test in CFA	141
Table 4.7	Reliability Statistics and Item-Total Statistics for factors of the EMSMM	142
Table 4.8	Perception of the EMSMM's factors based on respondents' designation	144
Table 4.9	Perception of the EMSMM's factors based on the trading area ...	145
Table 4.10	Factors' weights resulted from AHP analysis	147
Table 4.11	The factors of the EMSMM distributed according their importance and attributes, as resulted from the analyses	149
Table 5.1	KMO and Bartlett's Test – last run of factor analysis	158
Table 5.2	EFA with Varimax rotation results	159
Table 5.3	Results of the validity concern check for organizational performance	163
Table 5.4	Results of the validity and reliability test	164
Table 5.5	Results of relationship testing between the EMSMM's factors and organizational performance	170
Table 5.6	Results of relationship testing between the EMSMM and organizational performance	173
Table 5.7	Categories of organizational performance of shipping companies and their indicators, as resulted from the analyses.....	175
Table 6.1	Hypothesis test summary table	183

LIST OF FIGURES

Figure 1.1	Reported and attempted piracy attacks worldwide from 1993 to 2014.	4
Figure 1.2	Malacca Strait piracy incidents from 1995 to 2012	4
Figure 1.3	Structure of the thesis	11
Figure 2.1	Similarities between compulsory maritime security requirements for shipping companies	33
Figure 2.2	The Continuous Security Improvement (CSI) cycle	41
Figure 2.3	Deriving essential criteria for the EMSMM	48
Figure 2.4	Reported incidents involving stowaways from 2002 to 2009	54
Figure 3.1	Research process	79
Figure 3.2	Process of deriving the EMSMM's factors	81
Figure 3.3	Factors of the EMSMM	82
Figure 3.4	Process of deriving categories of organizational performance of shipping companies	97
Figure 3.5	Hypotheses tested in this study	100
Figure 4.1	An overview of the steps in an exploratory factor analysis	122
Figure 4.2	An overview of the steps of the AHP used in this study.....	123
Figure 4.3	Respondents' designation	126
Figure 4.4	Respondents' experience in the security related job or industry ...	126
Figure 4.5	Respondents' business sector	127
Figure 4.6	Location of the respondents' offices	127
Figure 4.7	Types of ships in operation of the respondents' companies	128
Figure 4.8	Types of management provided by the respondents' companies ..	128
Figure 4.9	Trading area of the respondents' companies	128
Figure 4.10	The EMSMM resulted from the CFA	136
Figure 4.11	Importance of the EMSMM's factors	147
Figure 5.1	Stages of the SEM	157
Figure 5.2	Categories of Business Performance resulted from the CFA	161
Figure 5.3	Results of the main SEM model with six independent and six dependent variables	167
Figure 5.4	Results of the main SEM model with one independent and six dependent variables	172

LIST OF ABBREVIATIONS

AEO, Authorized Economic Operator;
AHP, Analytic Hierarchy Process;
AIS, Automatic Identification System;
AMR, Advance Manifest Rule;
ANOA, Advance Notification of Arrival;
ANOVA, Analysis of Variance;
APEC, Asia-Pacific Economic cooperation;
BASC, Business Anti-Smuggling Coalition;
BCM, Business Continuity Management;
BCN, Biological, Chemical and Nuclear weapon;
BCP, Business Continuity Plan;
BCP, Business Continuity Planning;
CBA, Cost-Benefit Analysis;
CBP, US Customs and Border Protection;
CBF, Critical Business Functions;
CCTV, Closed-Circuit Television;
CFA, Confirmatory Factor Analysis;
CLF, Common Latent Factor;
CM, Crisis Management;
CSI, Container Security Initiatives;
CSI, Continuous Security Improvement;
CSO, Company Security Officer;
CSR, Continuous Synopsis Record;
CSM, Container Status Message;
C-TPAT, Custom-Trade Partnership against Terrorism;
DEA, Data Envelopment Analysis;
DM, Disaster Management;
EDI, Electronic Data Interchange;
EFA, Exploratory Factor Analysis;
EMSMS, Effective Maritime Security Management System;

ESM, Entry Summary Declaration;
EU, the European Union;
FROB, Freight Remaining on Board;
ILO, the International Labor Organization;
IMO, the International Maritime Organization;
ISO, the International Organization of Standardization;
ISPS Code, the International Ship and Port Facility Security Code;
ISSC, International Ship Security Certificate;
IT, Information Technology;
LTTE, Liberation Tigers of Tamil Eelam;
MPA, Maritime and Port Authority of Singapore;
MS, Merchant Ship;
MSM, Maritime Security Management;
MSMS, Maritime Security Management System;
MV, Merchant Vessel;
NOA, Notification of Arrival;
PDCA, Plan-Do-Check-Act Cycle;
PhD, Doctor of Philosophy;
PIP, Partners in Protection;
OECD, Organization for Economic Cooperation and Development;
QM, Quality Management;
RM, Risk Management;
ROA, Return on Assets;
ROI, Return on Investment;
RQ, Research Question;
RSO, Recognized Security Organization;
SAFE, Secure and Facilitate Global Trade;
SCS, supply chain security;
SCSMM, Supply Chain Security Management Model;
SEM, Structural Equation Modeling;
SID, Seafarer' Identity Documents;
SID Convention, the Seafarers' Identity Documents Convention;

SIN, Ship Identification Number;
SM, Security Management;
SMS, Security Management System;
SOLAS Convention, the International Convention for the Safety of Life at Sea;
SRQ, Sub-Research Question;
SSA, Ship Security Assessment;
SSAS, Ship Security Alert System;
SSO, Ship Security Officer;
SSP, Ship Security Plan;
STAR, Secure Trade in the APEC Region;
STP, Singapore Customs Secure Trade Partnership;
SUA Convention, Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation;
TQM, Total Quality Management;
TSM, Total Security Management;
URL, Uniform Resource Locator;
US, the United States;
US AMR, Advance Manifest Rule, The Presentation of Vessel Cargo Declaration to Customs Before Cargo is Laden Abroad Vessel at Foreign Port for Transport to the United States;
USD, United States Dollar;
VSP, Vessel Stow Plan;
WCO, the World Customs Organization;
24HR, 24 Hour Rule;
10+2 Rule, Ten plus Two Rule, Import Security Filing and Additional Carrier Requirements.

CHAPTER 1. INTRODUCTION

1.1. Scope

This PhD thesis presents a detailed research study on the effective management of maritime security in shipping companies. According to Onuoha (2009, p. 32), maritime security can be defined as:

the freedom from or absence of those acts which could negatively impact on the natural integrity and resilience of any navigable waterway or undermine the safety of persons, infrastructure, cargo, vessels and other conveyances legitimately existing in, conducting lawful transactions on, or transiting through territorial and international waterways.

In this study, the main focus is given to maritime security of merchant shipping, and therefore, the research scope is limited to shipping companies operating merchant ships. Threats to maritime security involving the mentioned companies are divided into direct and indirect (Moseley, 2009). Direct threats include transnational organized crime and illicit trafficking, terrorism, and piracy and armed robbery at sea. Indirect threats involve biological, chemical and nuclear (BCN) weapons, and corporate devices (for example, illegal access to information regarding the identity of vessels). The majority of regulations for shipping companies aiming to fight against the listed threats have an international nature, therefore the geographical scope of this study is not limited by any territorial framework and includes the companies worldwide.

1.2. Background Information

The problem in maritime security has existed for hundreds of years. Piracy, cargo pilferage, smuggling and stowaway were considered to be the main concerns because of the high frequency of occurrence. However, shipments of weapons of mass destruction as well as a movement of terrorists are also the threats that deserve a high importance because of their possible consequences. As discussed earlier, direct threats to maritime security can be classified as following:

Movement of terrorists and their means of financing. A terrorist act can be damaging to a society. Not only can it cause economical damages, but also might lead to great social and physical disruptions (Moseley, 2009). Shipping industry provides one of the possible modes for movement of terrorists and their means. It is believed that al Qaeda has some freighters under its control, which would allow an escape of people by sea as well as a shipment of bombs, operatives, commodities and money (Borger J. and Whitaker B. (2003) in Roach, 2004).

Piracy and armed robbery at sea. This threat is originated by “attacks particularly against merchant shipping in transit and in port by hijacking, homicide, robbery and theft” (Roach, 2004, p. 43). The main difference between the definitions of piracy and armed robbery at sea is that in a case of a former accident the attack is conducted from another vessel, whereas for the second one the involvement of at least two ships is not necessary (Moseley, 2009). A higher concentration of these accidents is reported in South-East Asia, Far East, West and North-East Africa, coasts of India, and some ports of South-America. This threat often causes great financial and operational problems for different parties of the international trade, and also impacts the global economy significantly (Fu et al., 2010).

Drug smuggling by sea. The global drug problem is an essential issue, which can harm social, economical and political stability and public health and safety (Moseley, 2009). Since “a substantial proportion of the total quantity of drugs seized is confiscated from maritime modes of conveyance or has been transported by sea” (Roach, 2004, p. 43), drug smuggling is another serious maritime security threat, which needs to be mentioned.

Migration by sea. This activity is facing not only the problem of illegal transportation of people, but also the issue of their safety, since the ferries are often overloaded. It is estimated that about four million people migrate by sea yearly, which results in billions of illegal profit (Roach, 2004).

Human trafficking. Human trafficking is associated with illegal transportation of people, when the victim was taken in a country of origin and transported to a country of destination with a purpose of receiving of payment or obtaining other benefits through control or exploitation of the victim. This type of criminal activity

“can lead to social degradation which has economic consequences from the perspective that legitimate local and foreign investment may suffer and decline” (Moseley, 2009, p. 19).

The indirect threats to maritime security include biological, chemical and nuclear (BCN) weapons and corporate devices.

Shipment of weapons of mass destruction. It is also believed that the weapons of mass destruction (WMD) might be transported by sea in a similar way as terrorists’ operatives (Roach, 2004). However, ships might be used not only for transporting BCN weapons, but also for performing a terrorist attack. “The use of a ship to carry out a terrorist act using these weapons would be several times more devastating, physically, socially and economically than a terrorist act committed with conventional weapons” (Moseley, 2009, p. 22).

Corporate devices. In the context of maritime security, this threat is associated with the difficulties to trace illegal activities, organisations and individuals caused by institutional devices and mechanisms. Precisely, it is often difficult to determine the owner of the vessel because of a multi-level structure of her ownership and commercial management. Besides, the fact that the ship registries do not have standardised regulatory procedures is another root cause of the threat (Moseley, 2009).

For a long time, there were no legal ways to deal with these problems. Different international and national organizations have been trying to improve the situation by introducing distinguished rules and conventions. For example, International Maritime Organization (IMO) adopted the International Convention for the Safety of Life at Sea (SOLAS) in 1974 and the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA Convention) in 1988, which came into force in 1992 (IMO, 1974, 1988). However, the piracy problem continued to grow. As can be seen from Figure 1.1, during the period from 1993 to 2000, the number of reported piracy attacks worldwide increased by almost 5 times. Figure 1.2 also shows a significant increase in a number of security incidents in Malacca Strait. Apart from the piracy issue, the possibility of ships being hijacked was also high. A cruise ship MS Achille Lauro was hijacked by members of Palestine Liberation Front in October 1985. Table 1.1 shows the list of

ships hijacked by Liberation Tigers of Tamil Eelam (LTTE) in a period from 1995 until the end of the organization's operational activity.

Figure 1.1 Reported and attempted piracy attacks worldwide from 1993 to 2014
Source: IMB (various years)

Figure 1.2 Malacca Strait piracy incidents from 1995 to 2012
Source: Pristrom et al. (2013)

Table 1.1 List of ships hijacked by LTTE from 1995 till 2009

Date	Hijacked ship
August 1995	Irish Mona
August 1996	Princess Wave
May 1997	Athena
July 1997	Misen
July 1997	Morong Bong
September 1997	MV Cordiality
August 1998	Princess Kash
May 1999	MV Sik Yang
July 1999	Newko
June 2000	Uhana
March 2003	Fuyuan Ya 225
December 2006	MV Farah III
January 2007	City of Liverpool

Source: Jayawardane (2009), Ministry of Defence, Sri Lanka (2009)

Moreover, the number of incidents involving stowaways and illegal migrants has risen significantly by the year 2000 (Chen, et al, 2005). There was a clear need for a stricter maritime security regime. Some new documents and amendments to existing conventions were already under consideration when several terrorist attacks, such as the bombings of the U.S.S. Cole in 2000 and the French oil tanker Limburg in 2002, made maritime security a hot issue in the international maritime agenda. These maritime terrorist attacks and the 9/11 attacks in 2001 have focused global attention on security threats, including maritime threats. Within a short period of time after this event, a lot of new regulations, including the International Ship and Port Facility Security Code (ISPS Code) (IMO, 2002), came into force.

The variety of the root causes and different nature of maritime security threats, as well as the wide range of the possible consequences of security incidents, including their economical and political significance, have lead to a high number of the regulations in this area. Firstly, every government is trying to address the problems in the way that is corresponding to other regulations of this government, by introducing the measures against security accidents, which are consistent with other internal country/region procedures and practices. Secondly, as discussed

earlier in this section, maritime security threats have very different origin, aims, concepts and consequences, and therefore require to be addressed differently. Thirdly, because of the multinational structure of the shipping business, there are a lot of distinguished bodies and organizations, as well as national governments, unions of countries and industry representatives, introducing relevant regulations. Based on all mentioned reasons, nowadays, there are a significant number of conventions, codes, standards, programs, and other documents regulating maritime security, which impose a long list of compulsory and voluntary requirements on shipping companies.

1.3. Research Problems, Aims, Questions and Objectives

The variety of maritime security threats and different ways to approach them resulted in the diversity of maritime security regulations, which subsequently poses a very important problem for shipping companies - how to meet and maintain the requirements while not jeopardizing other organizational performance. Besides the benefits expected from the implementation of these requirements, it also has negative impacts on organizational performance of companies, including extra expenses, additional manpower, paperwork, etc. (Thibault et al, 2006; Thai, 2007; Urciuoli et al, 2010; Yang, 2010). For some companies, additional cost related to security implementation has resulted in bankruptcy (Voort et al, 2002). Additionally, benefits expected from the implementation of maritime security regulations have not been fully obtained by shipping companies (Voss, et al., 2009).

There is a number of sources available, providing an information on negative impacts of security accidents. For example, Fu et al. (2010) provide a wide overview and the calculation of the economical impacts of the maritime piracy in Somalia area on global economic development. However, companies' managers still do not clearly understand how the introduced security requirements can help in the prevention and recovery from a terrorist attack, since available information on these attacks is very limited (Thibault, et al., 2006; Yang, 2010; Urciuoli, et al., 2010). The misunderstanding of benefits, as well as the achievement of negative results, may jeopardize the implementation of security regulations in shipping

companies (Peleg-Gillai et al., 2006; Thibault, et al., 2006; 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 without jeopardizing other organizational performance; in other words, how to achieve a good balance between security implementation and its impacts (Gould, et al., 2010; Hintsa, et al., 2009; Williams, et al., 2008).

However, there are not many studies that have been conducted to investigate the impacts of security management on organizational performance of shipping companies, even though the knowledge in this area would be beneficial and useful for the shipping industry. Besides, there is still no specific methodology or scale to measure the impacts of security implementation on organizational performance of shipping companies, which makes it difficult for them to understand the effectiveness of security management. Thus, the lack of such a methodology represents a key research niche, which this present study aims to address.

Based on the discussed problems, three aims of this research work have been identified. The primary aim in this study is to develop and validate an effective maritime security management model (EMSMM), which helps shipping companies implement compulsory and voluntary security requirements without jeopardizing other organizational performance. To develop the EMSMM, existing maritime security regulations and requirements imposed on shipping companies will be studied and analyzed. This represents the second aim stated in this research. The third aim is to explore the impacts of maritime security management on the organizational performance of shipping companies. To achieve this, the scale for performance measurement in shipping companies will be developed. For this purpose, the organizational performance of the companies will be analyzed and categorized.

To achieve the aims of this study, several research questions should be answered. This thesis has three main research questions corresponding with the aims. Each of them has several sub-questions. The research objectives explain what exactly should be done to answer the stated research questions. Table 1.2 provides the aims, research questions and research objectives of this study.

Table 1.2 Research aims, questions and objectives

Aims	Research Questions	Research Objectives
To study maritime security regulations and requirements for shipping companies.	<p>RQ1. What are the existing maritime security regulations and requirements for shipping companies?</p> <p>SRQ1.1 What regulations currently exist in the field of maritime security?</p> <p>SRQ1.2 What maritime security requirements are imposed on shipping companies?</p> <p>SRQ1.3. What maritime security requirements are implemented in shipping companies?</p>	<ul style="list-style-type: none"> - To review regulatory documents containing security requirements for shipping companies; - To compose a list of compulsory and voluntary maritime security requirements for shipping companies; - To explore implementation of these requirements in shipping companies.
To develop and validate the EMSMM for shipping companies.	<p>RQ2 How can maritime security be managed effectively in shipping companies?</p> <p>SRQ2.1 What management approaches and models are applicable to manage maritime security effectively?</p> <p>SRQ2.2 What problems of security management do shipping companies currently face?</p> <p>SRQ2.3 What are the essential criteria for the EMSMM?</p> <p>SRQ2.4 What are the factors of the EMSMM?</p>	<ul style="list-style-type: none"> - To review existing approaches and proposed systems, models and frameworks of security management; - To identify problems of security management in shipping companies; - To compose a list of essential criteria of the EMSMM; - To develop and validate the factors of the EMSMM.
To understand the impacts of maritime security implementation on organizational performance of shipping companies.	<p>RQ3 What are the impacts of maritime security management on organizational performance of shipping companies?</p> <p>SRQ3.1 What are the reported and proposed impacts of implementation of maritime security initiatives on organizational performance of shipping companies?</p> <p>SRQ3.2 How do the EMSMM and its factors impact organizational performance of shipping companies?</p>	<ul style="list-style-type: none"> - To review and summarize the impacts of implementation of maritime security initiatives on organizational performance of shipping companies; - To develop and validate categories and indicators of organizational performance of shipping companies for a purpose to measure impacts of security management; - To test the relationship between the EMSMM's factors and categories of organizational performance.

1.4. Research Methods

To achieve the discussed aims and objectives as well as to answer the formulated research questions, the methods of primary and secondary data analysis were used in the study. The secondary information was collected from various sources, including scientific and industrial publications, compulsory and voluntary regulatory documents, reports prepared by industrial, governmental and research institutions, and other sources. The primary data were collected through in-depth interviews with industry professionals in Singapore and two surveys, which sampling population included shipping and ship management companies worldwide.

The analysis of the collected information was conducted through various methods. To address the RQ1 and some of the sub-questions of the RQ2 and RQ3, the secondary data analysis based on the literature review was conducted. To answer the second research question regarding the effective maritime security management in shipping companies, three different methods of primary data analysis were applied, namely an Exploratory Factor Analysis (EFA), a Confirmatory Factor Analysis (CFA) and an Analytical Hierarchy Process (AHP). The third research question on the impacts of maritime security management on organizational performance of shipping companies was addressed through the following methods of primary data analysis: the EFA, the CFA and Structural Equation Modeling (SEM). Besides, for all three research questions the qualitative information, collected through interviews and surveys, was manually analysed based on content and thematic analysis.

The combination of variety of is essential and necessary in this study, since the addressed questions have not been answered before and the mentioned problems have not been widely studied. Therefore, both secondary data analysis through comprehensive literature review and primary data analysis through conducting interviews and surveys have been applied in this study.

1.5. Structure of the Thesis

This thesis is structured into six chapters. Following the brief introductory Chapter 1, Chapter 2 provides detailed and comprehensive literature review on several subjects of the study, namely the security regulations and requirements for shipping companies and security management and its impacts on their organizational performance. Chapter 3 presents the methodology for this research, including the research questions of the study, research approach and flow, process of model building, data collection methods, and analytical techniques. The analyses and results are provided in Chapters 4 and 5. Chapter 4 presents the analysis of the data on the EMSMM. As discussed in the previous section, the analyses were conducted through three different methods, namely an EFA, a CFA and an AHP. Chapter 5 describes the impacts of maritime security management on organizational performance of shipping companies. The methods applicable in this chapter include the EFA, the CFA and SEM. The last chapter of the thesis provides an overview of the results, managerial and academic implications, research limitations and possible future research directions. A diagram of the structure of this thesis is presented in Figure 1.3.

Chapter 1 INTRODUCTION	<ul style="list-style-type: none"> • Scope • Background Information • Research Problems, Aims, Questions and Objectives • Research Methods • Structure of the Thesis
Chapter 2 LITERATURE REVIEW	<ul style="list-style-type: none"> • Introduction • Maritime Security Regulations and Requirements for Shipping Companies • Effective Maritime Security Management in Shipping Companies • The Link between Maritime Security and Organizational Performance of • Summary of Literature Review
Chapter 3 METHODOLOGY	<ul style="list-style-type: none"> • Introduction • Research Questions • Research Approach • Research Process • Model Building and Hypotheses Development • Data Collection • Errors and the Ways Used to Reduce Them • Summary
Chapter 4 EFFECTIVE MARITIME SECURITY MANAGEMENT IN SHIPPING COMPANIES	<ul style="list-style-type: none"> • Introduction • Methods of Data Analysis • Respondents Profile • Perception of the EMSMM in Shipping Companies • Measurement Validity and Reliability Analysis • Perception of the EMSMM's Factors based on the Respondents' Designation and Trading Areas of Their Companies • Relative Importance of the Factors of the EMSMM: Perception of Nine Experts • Discussion • Summary
Chapter 5 IMPACTS OF MARITIME SECURITY MANAGEMENT ON ORGANIZATIONAL PERFORMANCE OF SHIPPING COMPANIES	<ul style="list-style-type: none"> • Introduction • Methods of Data Analysis • Relationship between Implementation of the EMSMM and Organizational Performance • Discussion • Summary
Chapter 6 DISCUSSIONS AND CONCLUSIONS	<ul style="list-style-type: none"> • Introduction • Discussion of the Findings • Implications • Research Limitations • Future Research

Figure 1.3 Structure of the thesis

CHAPTER 2. LITERATURE REVIEW

2.1. Introduction

The purpose of this chapter is to present a review of literature on the management of maritime security in shipping companies. According to the aims of the study, the chapter is organized into three sections. The first section provides a review of the regulations and requirements imposed on shipping companies and other supply chain companies for the purpose of increasing security. The literature in this section mostly contains legal documents, standards, guidance and other regulations relevant to the topic, as well as industry reports and reviews. The second section of the chapter provides a review of literature on the management of maritime security in shipping companies. Firstly, it reviews the existing management approaches, frameworks and models of security management. Then, it discusses the current problems of security management in shipping companies. Finally, based on the discussed approaches and existing problems, a list of essential criteria for the EMSMM in shipping companies is presented. The third section reviews a literature on the impacts of security management on organizational performance of shipping companies. For this purpose, the literature on organizational performance is first reviewed, followed by studies on the impacts of security management on organizational performance. In addition, various classifications of the impacts are presented. The chapter ends with a summary of the literature review and a discussion on the gaps and ways to fill them.

2.2. Maritime Security Regulations and Requirements for Shipping Companies

As a part of maritime law, maritime security regulations have a very diverse nature. This section aims to discuss maritime security regulations for shipping companies, which are introduced by international and national governments and by industry organizations. It also aims to study the security requirements imposed on the companies, as well as their implementation and effectiveness.

2.2.1. Maritime Security Regulations

The maritime security requirements for shipping companies are found in various sources. In some literature, these sources are divided into three sets (Bichou et al., 2007; Bichou et al., 2014; Gutierrez and Hintsa, 2006; Talley, 2008; Papa 2013). The first set includes regulations proposed by different international organizations. A prevailing legal document regulating maritime security is the International Ship and Port Facility Security Code (ISPS Code) (IMO, 2002). It came into force on 1 July 2004, together with other amendments of SOLAS Convention, and imposed a list of compulsory requirements on shipping companies and ships, engaging in international voyage. The IMO (IMO Website) characterises the ISPS Code as following:

a comprehensive set of measures to enhance the security of ships and port facilities, developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks in the United States.

The Code was introduced through Chapter XI-2 in SOLAS “Special measures to enhance maritime security”. It contains two parts, mandatory and recommendatory.

The Seafarers’ Identity Documents Convention is another document from this set, requiring every seafarer to have a seafarers’ identity document (ILO, 2003). The Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework), a program developed by World Customs Organization (WCO) based on the contractual relationship between Customs and supply chain participants, aims to enhance the facilitation and security of international trade (WCO, 2007).

The second set of maritime security initiatives was introduced at the national and regional levels. It includes states’ national regulation, as well as programs, rules or agreements developed by unions of countries. This set contains a mix of mandatory regulations and voluntary programmes, each of which is consistent with international legislation. The most significant documents of the second set were introduced in the United States (US), the European Union (EU) and Asia-Pacific Economic Cooperation (APEC) Region. After the terrorist attack in September 2011, the US government started a very aggressive policy for the protection of the

national security. Since then a lot of new security regulations have been developed and implemented in different areas of security, *inter alia*, maritime security. Specifically, the Presentation of Vessel Cargo Declaration to Customs before Cargo is Laden Abroad Vessel at Foreign Port for Transport to the United States (AMR) is a rule, developed in addition to the Container Security Initiative (CSI), and compulsory applicable to all US-bound cargo (CBP, 2002; DoT, 2002). Import Security Filing and Additional Carrier Requirements (10+2 Rule) is another cargo security initiative of the US that requires all carriers to submit additional information about the cargo to the US Customs before entering the US port (CBP, 2009). Additionally, Advance Notice of Arrival (ANOA) is a mandatory US requirement, aiming to select high risk ships before their arrival to US port (DHS, 2003). In addition, the Custom-Trade Partnership against Terrorism (C-TPAT) is a voluntary agreement between the US Customs and businesses involved in the shipping of goods to the US and was launched in 2001 (CBP, 2001). Similar to WCO Framework of Standards, C-TPAT contains the requirements for businesses willing to enter into a contracting relationship with the US Customs and enjoy the offered benefits. Although the participation in C-TPAT is not compulsory for port operators and shipping companies, some authors believe that “the security recommendations will eventually become the actual requirements” (Banomyong, 2005, p. 10).

Simultaneously with the US attempts to enhance transport security, the EU also increased its activity in developing new regulations and voluntary programs. In 2004, the EU introduced Regulation on enhancing Ship and Port Facility Security (EU, 2004) that transported into EU law a mandatory part A of the ISPS code and Chapter XI-2, and made some paragraphs of Part B compulsory for Member States. It also widened a list of ships and port facilities, to which the regulation applies, by adding domestic shipping operators and port facilities serving them. As a part of WCO SAFE Framework of Standards, the European Commission developed a set of measures to accelerate the implementation of security related requirements, including the Authorised Economic Operators program (EU, 2007). Besides, the EU Advance Cargo Security Rules (EU 24HR) requires carriers to submit the cargo related information to port authorities of contracting states before loading in foreign

ports or before arrival (EU, 2011). Similar rules exist in China, Canada and Mexico regulations. Besides, the second set also includes the Secure Trade in the APEC Region (STAR) Initiative that aims to enhance security and efficiency in the APEC region's seaport, airports and other access points (APEC, 2002). Moreover, similar to WCO Framework and C-TPAT, some countries have introduced security programs based on voluntary partnership with the private sector. Among them are Singapore Customs Secure Trade Partnership (STP) Program (Singapore Customs, 2011), Partners in Protection (PIP) in Canada (CBSA, 1994), StairSec in Sweden, New Zealand Secure Export Partnership (Customs Service, 2003), and others.

Some voluntary initiatives developed by industry players form a third set of maritime security regulations. Among them is the ISO's "Specification for Security Management System for the Supply Chain", which was developed as guidance for organizations to manage security and implement necessary security measures in the effective manner (ISO, 2007). Similarly, the International Business Anti-Smuggling Coalition (BASC) Standards have been developed by World BASC Organization and serve as a guideline for the implementation of security measures (BASC, 2002).

Regulations from the three sets as listed above can also be classified according to their mandatory and voluntary nature. Mandatory regulations contain compulsory requirements in terms of implementation. These requirements may be compulsory for all members of the shipping industry, regardless of their area of operation, or only for those operating in a specific region or under specific conditions. Meanwhile, the requirements of voluntary nature are not compulsory for implementation. However, as several authors believed, some of them may eventually become a minimum criterion for participating in international trade, as non-compliance often has a negative effect on business performance of the shipping companies (Altemöller, 2011; Banomyong, 2005; Gutierrez and Hintsa, 2006; Metaparti, 2010; Papa, 2013; Rice and Spayd, 2005). Table 2.1 shows two groups of maritime security regulations: regulations imposing compulsory security requirements and those containing voluntary recommendations.

Table 2.1 Maritime security regulations for shipping companies

Set of Regulations	Regulations containing compulsory requirements	Regulations containing voluntary requirements
International	<ul style="list-style-type: none"> • ISPS Code, • Seafarers' Identity Documents (SID) Convention 	<ul style="list-style-type: none"> • SAFE Framework of Standards
National and regional	<ul style="list-style-type: none"> • AMR (<i>*for all cargo bound to US</i>), • 10+2 Rule (<i>*for all cargo bound to US</i>), • ANOA (<i>*for all cargo bound to US</i>), • EU Regulation on Enhancing Ship and Port Facility Security (<i>*all EU Member States</i>), • EU 24HR (<i>*for all goods that are arrived to EU countries, Norway, Switzerland</i>), • Canada 24HR (<i>*for cargo bound to Canada</i>), • China 24HR (<i>*for cargo bound to China</i>), • Mexico 24HR (<i>*for cargo bound to Mexico</i>) 	<ul style="list-style-type: none"> • C-TPAT, • EU AEO, • STAR initiatives, • PIP, • STP, • StarSec, • Secure Export Partnership
Industry	<i>No regulations containing compulsory requirements have been originated by industry</i>	<ul style="list-style-type: none"> • ISO Standards, • BASC

Notes: * indicates area of application.

Abbreviations: AEO – Authorized Economic Operator; AMR – Advance Manifest Rule; ANOA – Advance Notification of Arrival; BASC – Business Anti-Smuggling Coalition; C-TPAT – Custom-Trade Partnership against Terrorism; ISO – the International Organization of Standardization; ISPS – International Ship and Port Facility Security Code; PIP – Partners in Protection; SAFE – Secure and Facilitate Global Trade; STAR – Secure Trade in the APEC Region; STP – Singapore Customs Secure Trade Partnership; 24HR – 24 Hour Rule.

2.2.2. Maritime Security Requirements

2.2.2.1. Classification of Maritime Security Requirements

The regulations listed in Table 2.1 impose a long list of requirements on shipping companies. There were several attempts made by the industry and scientists to classify the requirements. A significant number of regulations and voluntary programs, aiming to enhance maritime and supply chain security, contain requirements or recommendations divided into categories (APEC, 2002; BASC, 2002; CBP, 2001; EU, 2007; ISO, 2007; Singapore Customs, 2011; WCO, 2007). The number of categories varies from six to thirteen. Moreover, several authors have also been trying to make some classifications. For instance, Gutierrez and Hintsa (2006) proposed a general supply chain security management framework consisting of 25 security measures classified into five categories: facility

management, cargo management, human resources management, information management, and business network and company management systems. Yang (2010) mentioned in his paper nine categories as generally included in supply chain security: physical security, access control, personnel security, education and training awareness, procedural security, documentation processing security, trading partner security, conveyance security, and crisis management and disaster recovery. Thai and Grewal (2007) listed in their paper six key security dimensions such as security awareness education and training, access control, physical security, procedural security, personnel security, and information security. This method of organizing security measures is often called the layered approach. In the US National Strategy for Maritime Security (DoT, 2005), the layered approach was defined as follows:

Layered approach to maritime security means that security measures are applied in different points of vulnerability: transportation, staff, passengers, conveyance, access control, cargo and baggage, ports, and security en route.

Different sources propose different numbers of categories of maritime security requirements. For the purpose of this research, they were classified into ten categories, namely, *Physical security, Access control, Personnel security, Cargo security, Security training and awareness, Information and documentation security, Cooperation with authorities, Security of business partners, Crisis management and incident recovery, and Security assessment, response and improvement.*

Some of these categories intersect with one another, that is why it is difficult to clearly distinguish between them and, therefore, some requirements may be simultaneously put into several categories. For example, under the ISPS Code, requirements to design Company Security Officer (CSO) for every company and Ship Security Officer (SSO) for every ship may be stated in several categories, because their duties should include many aspects of security (IMO, 2002). Moreover, the development, implementation and continuous improvement of Ship Security Plan (SSP) are a compulsory requirement for every ship (IMO, 2002). The SSP might also be considered under different categories. The description of each security category and measures included are given as follows.

Physical security

The category of *Physical security* includes security measures that control the facility's interior zones and exterior perimeters. Physical security requirements include compulsory requirements under the ISPS Code: CSO, SSO, SSP, Ship Security Alert System (SSAS), Automatic Identification System (AIS) and Ship's identification number (SIN). Under this category, the duties of CSO will include ensuring the implementation of security requirements and their consistency with safety requirements; SSO shall ensure that appropriate security measures are maintained and coordinate the security aspects of the ship's stores and equipment (IMO, 2002). SSP shall contain measures to prevent weapons, dangerous substances and devices from being taken on board the ship, identify restricted areas, Ship Security Alert System (SSAS) and its activation points (IMO, 2002).

Moreover, several security related documents, such as WCO SAFE Framework of Standards, C-TPAT, AEO Program, and STAR initiatives provide that physical requirements include security measures, related to aspects such as external boundaries of premises, building structure, external and internal windows, fencing, gates and gateways, locking devices, lighting, key control, parking, cargo storage areas, alarm systems, video surveillance cameras and/or closed circuit television (CCTV), internal physical security measures, mail service security, warning signs, markings, barriers and access control points, physical security policy manual and procedures (APEC, 2002; CBP, 2001; EU, 2007; WCO, 2007).

Access control

In the second category, *Access control* prohibits unauthorized access to facilities, vessels, loading docks, cargo areas and conveyances. Security requirements under this category include, among others, SSP (IMO, 2002) and Seafarers identity document (SID) issued by a Member State for every crew member (ILO, 2003). As a requirement of the ISPS Code, SSP shall include measures for the prevention of unauthorized access to the ship. Paragraph 9.9 of Part B of the ISPS Code states that the SSP should establish the security measures covering all means of access to the ship, such as ladders, gangways, ramps, doors, side scuttles, windows and ports, mooring lines and anchor chains, crane and hosting gears.

The category of *Access control* includes some non-mandatory security requirements imposed by different documents: (i) procedures for positive identification of employees, visitors and vendors at all points of entry; (ii) procedures to identify, challenge and address unauthorized person; (iii) procedures to deny access and trigger an alarm when visitors attempt to enter an unauthorized area; (iv) control of the times individuals have access to facilities; (v) map of restricted areas within the view of employees and visitors; and (vii) inspection of persons and packages (APEC, 2002; BASC, 2002; CBP, 2001; Singapore Customs, 2011; WCO, 2007).

Personnel security

The category of *Personnel security* includes security measures for personnel selection and hiring, screening of current and prospective employees, and procedures for retaining them. As a requirement of Seafarers Identity Documents Convention, it is compulsory for every seafarer to hold a valid SID (ILO, 2003). Other requirements of this category imposed by different regulations include procedures for screening of current and prospected employees, implementation of drug consciousness programs, drug and alcohol testing, employee identification procedure, procedures for hiring, induction, retaining and termination of employees, assuring correct alignment of job skill requirements with individual's skills, periodical review of current positions (APEC, 2002; BASC, 2002; CBP, 2001; ISO, 2007; Singapore Customs, 2011; WCO, 2007). Additionally, C-TPAT contains some more requirements for personnel security, such as the procedure for identification of the potential risk of desertion/absconding and masters' account for all crewmen to CBP, prior to the vessel's departure to the US ports (CBP, 2001).

Cargo security

The fourth category of *Cargo security* refers to requirements ensuring the security of cargo, appropriate sealing and inspection of containers, security of personnel working with cargo, security of access and storage of cargo, and cargo security related information. Part B of the ISPS Code provides security measures during the handling of cargo to prevent tampering and to prevent inappropriate cargo from being loaded onboard the ship (IMO, 2002), such as routine checking of cargo, cargo transport units and cargo spaces; checks to ensure that cargo matches

the documentation; search of vehicles before loading onboard car-carriers, ro-ro and passenger ships; visual and physical examination; using of scanning/detection equipment, mechanical devices or dogs; and possible off-site checking and sealing of cargo when regular cargo movement are in place.

Other security regulating documents list the following requirements of *Cargo security*: (i) security policy manual or guidance to preserve the integrity of the cargo; (ii) written procedure for sealing of cargo to be used by the shipping companies and their business partners; (iii) procedure for recognizing and reporting compromised seals and/or containers to Customs administration; (iv) ensuring that only designed personnel seals are used and safeguard the cargo; (v) regular examination of security and control procedures to ensure that authorized personnel can handle the cargo properly and to prevent unauthorized persons from access to the cargo; (vi) procedures for reporting detected unauthorized access to the cargo and storage areas; (vii) procedure to manage, secure and control all cargo during storage, transportation, loading and unloading; (viii) ensuring the security of cargo information, both manual and electronic; (ix) positive identification of drivers/persons receiving or delivering the cargo; and (x) seven-points procedure for the inspection of full and empty containers recommended by WCO SAFE Framework of Standards and Singapore Customs STP: front wall, left side, right side, floor, ceiling/roof, inside/outside doors, outside/undercarriage (BASC, 2002; CBP, 2001; Singapore Customs, 2011; WCO, 2007).

Security training and awareness

The category of *Security training and awareness* includes measures to educate personnel regarding security policies, increase security awareness in the company and understanding the consequences of unauthorized actions. The ISPS Code requires shipping companies to organize periodical training, drills and exercises on ship security. According to Part B of the Code, SSO, CSO and appropriate shore-based personnel should have knowledge of security administration, relevant international conventions, codes and recommendations, relevant Government legislation and regulations, responsibilities and functions of other security organizations, methodology of ship security assessment, methods of ship security surveys and inspections, ship operations and conditions, ship security measures,

emergency preparedness and response and contingency planning, instruction techniques for security training and education, including security measures and procedures, handling sensitive security related information and security related communications, knowledge of current security threats and patterns, recognition and detection of weapons, dangerous substances and devices, recognition, on a non discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security, techniques used to circumvent security measures, security equipment and systems and their operational limitations, methods of conducting audits, inspection, control and monitoring, methods of physical searches and non-intrusive inspections, security drills and exercises, including drills and exercises with ships.

In addition, the SSO should have adequate knowledge of the layout of the ship, the ship security plan and related procedures, crowd management and control techniques, operations of security equipment and systems, and testing, calibration and, whilst at sea, maintenance of security equipment and systems. Moreover, shipboard and facility personnel having specific security duties should have sufficient knowledge, such as knowledge of current security threats and patterns, recognition and detection of weapons, dangerous substances and devices, recognition of characteristics and behavioural patterns of persons who are likely to threaten security, techniques used to circumvent security measures, crowd management and control techniques, security related communications, knowledge of the emergency procedures and contingency plans, operations of security equipment and systems, testing, calibration and, whilst at sea, maintenance of security equipment and systems, inspection, control, and monitoring techniques, and methods of physical searches of persons, personal effects, baggage, cargo, and ship's stores. All other shipboard personnel should have sufficient knowledge of and be familiar with relevant provisions of the SSP, including the meaning and the consequential requirements of the different security levels, knowledge of the emergency procedures and contingency plans, recognition and detection of weapons, dangerous substances and devices, recognition, on a non discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security, and techniques used to circumvent security measures. The

objective of drills and exercises is to ensure that the shipboard and port facility personnel are proficient in their security duties.

Besides requirements of the ISPS Code, security requirements of this category are contained in other regulations, such as WCO SAFE Framework of Standards, C-TPAT, ISO Standards, BASC Standards, STAR Initiatives, Singapore Customs STP (APEC, 2002; BASC, 2002; CBP, 2001; ISO, 2007; Singapore Customs, 2011; WCO, 2007). They include (i) procedures to make personnel aware of the importance of compliance with the security management policy; (ii) procedures to make personnel aware of their roles, responsibilities and daily tasks; (iii) keeping of records of competence and training; (iv) procedures to educate, where appropriate, trading partners regarding security policies; (v) provision of educational material, expert guidance to all relevant personnel; and (vi) use of press releases, email distribution lists and bulletin boards.

Information and documentation security

The category of *Information and documentation security* includes security measures to protect electronic and manual documentation from unauthorized access, loss or changing of data. The ISPS Code requires SSP and records of activities shall be protected from unauthorized access, disclosure, deletion, destruction or amendment (Pallis, 2006). Non-mandatory requirements under this category imposed by other security regulating documents include (i) insuring confidentiality of commercial and security sensitive information, including limited access to data or information and having secure areas for storage and filing; (ii) establishing and implementation of security management documentation system, that includes security policy, objectives and targets, description of the scope and main elements, and references to related documents; (iii) establishing and implementation of procedures for controlling all documents, data and information; (iv) establishing the rules for employees not to divulgate security related information, such as information about security training, access control system, locations of security or communication equipment; (v) maintaining documented information security policy and procedures and security related controls to protect the electronic system from unauthorized control; (vi) implementing procedures and back-up capabilities to protect against the loss of information; (vii) using international standards developed

regarding electronic data structure, timing for submission and message content; (viii) ensuring periodic change of password for password protection; (ix) keeping a system to identify the abuse of IT and appropriate disciplinary actions for abuse; (x) securing cargo related documents; (xi) establishing of signature and stamp policies; (xii) establishing of deadlines for processing of documents; and (xiii) exercising special control for emergency/last minute shipment information (APEC, 2002; BASC, 2002; CBP, 2001; ISO, 2007; Singapore Customs, 2011; WCO, 2007).

Cooperation with authorities

The category of *Cooperation with authorities* includes compliance with national and international security regulations, consultation, co-operation and communication with appropriate authorities regarding security issues, and submission of required security information to authorities. The ISPS Code requires ships to undertake verification carried out by Administration and have an International Ship Security Certificate (ISSC), issued by Administration or recognized security organization (RSO) on behalf of Administration after verification, or in some cases Interim Ship Security Certificate. Additionally, every ship shall be issued with a Continuous Synopsis Record (CSR). CSR shall be issued by Administration, provide records of the history of the ship, be kept on board and be available at any time for inspection. Besides that, records of the following activities of the ship shall be kept on board and be available for access by a Contracting Government, including: training, drills and exercises, security threats and security incidents, breaches of security, changes in security level, communications related to the direct security of the ship such as specific threats to the ship or to port facilities where the ship is, or has been, internal audits and reviews of security activities, periodic review of the ship security assessment, periodic review of the ship security plan, implementation of any amendments to the plan, and maintenance, calibration and testing of any security equipment provided on board including testing of the ship security alert system.

Moreover, the Code requires every ship intending to enter the port of another Contracting Government to provide on the request of the officers the following information for the last 10 calls not less than 24 hours before entering into port: valid Certificate and issuing authority, current operating security level, operating

security level in last 10 ports of calling, any special security measures in last 10 ports of calling, appropriate security procedures were maintained in last 10 ports of calling, and other particular security related information. Additionally, this category includes the responsibility of the CSO to arrange the initial and subsequent verifications of the ship by the Administration or the RSO, and requirements for the SSP to contain procedures for responding to Government instructions and for interfacing with port facility security activities.

Under the requirements of the US AMR, all carriers of containerized and break bulk cargo bound to the US port shall submit cargo manifest (declaration) to the US Customs 24 hours before the related cargo is laden aboard the vessel at the foreign port (DoT, 2002). The declaration shall contain detailed information about the cargo, vessel and voyage including the foreign ports' names. Additionally, under "10 + 2" Rule, ocean carriers are required to provide two additional sources of data – Vessel Stow Plan and Container Status Message (CBP, 2009). The Vessel Stow Plan shall be submitted within 48 hours after the carrier's departure from the last foreign port and must contain elements about the cargo, vessel, equipment and voyage. The Container Status Message shall be submitted within 24 hours after the message is entered into the carrier's equipment tracking system. Moreover, the US Coast Guard requires ships calling to the US port to submit a 96-hour Notice of Arrival (ANOA) to select high-risk ships before their arrival (DHS, 2003).

Similar to ISPS Code and US ANOA, EU Regulation on enhancing Ship and Port Facility Security requires every ship entering the port of Member States to provide security relevant information to the Government at least 24 hours in advance (EU, 2004). Moreover, Maritime and Port Authority of Singapore (MPA) also requires ships to submit a Notification of Arrival prior to entering the port (MPA). Analogical to the US 24 Hour Manifest Rule, the EU Advance Cargo Security Rules require an Entry Summary Declaration (ESM) to be lodged for all deep sea containerized goods that are to arrive in the EU 24 hours before the vessel loading at the foreign port. The time may be reduced to four hours before arrival for deep-sea non-containerized cargo and to two hours before arrival for short sea cargo. Goods are to arrive in the EU include goods to be imported, transshipped, transited through the EU and Freight Remaining on Board (FROB) (EU, 2011).

Similar requirements are imposed for cargo bound to China, Canada, and Mexico (CBSA, 2004; China Customs, 2008; MCA, 2008)

Non-mandatory requirements under this category imposed by several documents include the following security measures: details of the links with relevant authorities and the necessary communication systems to allow effective communication; continuing mutual exchange of information with the authorities; and procedures for reporting to relevant authorities of any suspicious incidents, cargo, cargo documentation or requests for information (BASC, 2002; WCO, 2007).

Security of business partners

The category of *Security of business partners* indicates procedures for constant cooperation with trading partners, as well as procedures for the screening of current and prospective business partners. The term “business partners” includes service providers, suppliers, manufacturers, contractors and vendors (Singapore Customs, 2011). Security of business partners requirements include the extensive exchange of information with trading partners for enhanced security coordination and cooperation, mutual supply chain security policy, security education, training and awareness of and by trading partners, procedures for screening and selection of business partners, procedures to monitor and review business partners’ compliance to security requirements, business partners’ participation in supply chain security programmes administrated by foreign Customs, and mutual security agreements with trading partners (APEC, 2002; CBP, 2001; Singapore Customs, 2011; WCO, 2007).

Crisis management and incident recovery

The category of *Crisis management and incident recovery* involves advance planning and establishment of processes to operate under extraordinary circumstances. The concept of security levels introduced in the ISPS code may be classified in this category. According to IMO (2002), a ship is required to operate on security level set by the Contracting Government. There are three possible levels of security. Higher security levels indicate a higher possibility of security incidents: Security level 1: normal, the level at which the ship normally operates; Security level 2: heightened, the level applied for as long as there is a heightened risk of a

security incident; and Security level 3: exceptional, the level applied for the period of time when there is a probable or imminent risk of a security incident.

At security level 1, the following activities shall be carried out: ensuring the performance of all ship security duties, controlling access to the ship, controlling the embarkation of persons, monitoring of deck areas and areas surrounding the ship, monitoring restricted areas and ensure that only authorized persons have access, supervising the handling of cargo and ship's stores, and ensuring that security communication is readily available. Additional protective and further specific protective measures shall be implemented at security levels 2 and 3 respectively. Additionally, requirements of the ISPS Code on crisis management and incident recovery include duties of the SSO to report all security incidents to appropriate authorities. Besides that, the SSP shall include procedures for responding to security threats or breaches of security, procedures for evacuation in the case of security threats and procedures for reporting security incidents (IMO, 2002).

Other requirements of the category of *Crisis management and incident recovery* imposed by some voluntary regulations include: development and periodical testing and reviewing of contingency plans for emergency security situations and for disaster or terrorist incident recovery, procedures for identification of potential risks and responses to security incidents and emergency situations, development of crisis management rooms, periodic training on crisis management, incident tracking and information communication, investigation capability and follow-up, analysis of causes of crisis, and development of a Business Continuity Plan (BCP) to ensure that Critical Business Functions (CBF) can be continued during and after crisis or incident (APEC, 2002; ISO, 2007; Singapore Customs, 2011; WCO, 2007).

Security assessment, response and improvement

The last category of *Security assessment, response and improvement* includes procedures for periodical assessment of security management system, including security policy, security objectives, and threats and risks, as well as procedures for improvement and development of new strategies. The ISPS Code requires every ship to undertake periodical security assessment (IMO, 2002). Security assessment

can be carried out by persons with appropriate skills or by RSO. Ship security assessment (SSA) shall include the following elements: (i) identification of existing security measures, procedures and operations and their level of effectiveness in reducing vulnerability; (ii) identification and evaluation of key ship board operations/important asset and infrastructure that is important to protect; (iii) identification of possible threats to the key ship board operations/asset and infrastructure and the likelihood of their occurrence, in order to establish and prioritise security measures; and (iv) identification of weaknesses, including human factors in the infrastructure, policies and procedures.

Therefore, the CSO shall ensure that SSAs are carried out, the SSP is modified as appropriate, internal audits and reviews of security activities are arranged, and consistency is ensured between security requirements and safety requirements. The SSO shall undertake regular security inspection of the ship to ensure that appropriate security measures are maintained, maintain and supervise the implementation and amendment of SSP, report to the CSO any deficiencies identified during inspections, reviews, audits and verification of compliance. Besides, the SSP shall be developed and maintained based on the SSA. It will include procedures for auditing security activities and periodic review of the SSP.

Moreover, the category of *Security assessment, response and improvement* include security measures imposed by C-TPAT program, WCO SAFE Framework of Standards, ISO Standards, such as ensuring of integrity and adequacy of the security management system (SMS), identification of potential areas for improvement of the SMS, audits and evaluation of compliance with appropriate legal requirements, self-assessment procedures and identification of responsible parties, and follow-up actions from previous security reviews (CBP, 2001; ISO, 2007; WCO, 2007).

Based on the discussion above, Table 2.2 provides a summary of maritime security requirements classified into ten categories. The table also gives information on security regulations, which contain the requirements.

Table 2.2 Maritime security requirements for shipping companies

No	Category	Security requirements for shipping companies	
		Compulsory requirements and requirements compulsory under specific conditions (*conditions)	Voluntary requirements
1	Physical security	<ul style="list-style-type: none"> - CSO; - SSO, SSP; - SSAS; - AIS; - SIN (ISPS Code). 	<ul style="list-style-type: none"> - gates and gateways, - locking devices, - lighting, - key control, - alarm systems, - video surveillance cameras and/or closed circuit television (CCTV), - internal physical security measures, - mail service security, - warning signs, markings, barriers and access control points, - physical security policy manual and procedures <p>(WCO SAFE Framework of Standards, C-TPAT, AEO Program, STAR initiatives)</p>
2	Access control	<ul style="list-style-type: none"> - SSP (ISPS Code); - SID (SID Convention). 	<ul style="list-style-type: none"> - identification of employees, visitors, vendors; - access of vehicles, persons and goods; - access of unauthorized person; - denial of access and activation of an alarm when visitors attempt enter an unauthorized area; - control of the times of access to facilities; - map of restricted areas; - inspection of persons and packages <p>(WCO SAFE Framework of Standards, C-TPAT, AEO Program, STAR initiatives, STP, BASC).</p>
3	Personnel security	<ul style="list-style-type: none"> - SID (SID Convention). 	<ul style="list-style-type: none"> - screening of current and prospected employees; - drug consciousness programs; - drug and alcohol testing; - employee identification procedure; - procedures for hiring, induction, retaining and termination of employees; - assuring of correct alignment of job skill requirements with individual's skills; - periodical review of current positions;

			(WCO SAFE Framework of Standards, C-TPAT, AEO Program, STAR initiatives, STP, BASC, ISO Standards); - procedure for identification of the potential risk of desertion/absconding; - masters' account for all crewman to CBP prior vessel's departure to US ports (C-TPAT).
4	Cargo security	<ul style="list-style-type: none"> - routine checking of cargo, cargo transport units and cargo spaces; - checks to ensure that cargo matches the documentation; - search of vehicles before loading onboard car-carriers, ro-ro and passenger ships; - visual and physical examination; - using of scanning/detection equipment, mechanical devices or dogs; - possible off-site checking and sealing of cargo when regular cargo movement has place (ISPS Code). 	<ul style="list-style-type: none"> - security policy manual or guidance to preserve integrity of cargo; - written procedure for sealing of cargo; - procedure for recognizing and reporting compromised seals and/or containers to Customs administration; - ensuring that only designed personnel seals and safeguard the cargo; - regular examination of security and control procedures of cargo handling; - procedure to manage, secure and control all cargo during storage, transportation, loading and unloading; - security of cargo information, both manual and electronic; - seven-points procedure for inspection of full and empty containers (WCO SAFE Framework of Standards, AEO Program, C-TPAT, STP, BASC).
5	Security training and awareness	<ul style="list-style-type: none"> - periodical training, drills and exercises of CSO, SSO, appropriate shore-based and shipboard personnel (ISPS Code). 	<ul style="list-style-type: none"> - awareness of the importance of compliance with the security management policy; - roles, responsibilities and daily tasks of personnel; - records of competence and training; - education of trading partners; - educational material, expert guidance to all relevant personnel; - press releases, email distribution lists and bulletin boards (WCO SAFE Framework of Standards, C-TPAT, AEO Program, STAR initiatives, STP, BASC, ISO Standards).
6	Information and documentation security	<ul style="list-style-type: none"> - protection of the SSP and records of activities from unauthorised access (ISPS Code). 	<ul style="list-style-type: none"> - the confidentiality of commercial and security sensitive information; - security management documentation system, that includes security policy; - procedures for controlling all documents, data and information; - rules for employees not to divulgate security related information; - documented information security policy and procedures and security related controls - procedures and back-up capabilities to protect against the loss of information; - international standards developed regarding electronic data structure, timing for submission and message content; - password protection;

			<ul style="list-style-type: none"> - system to identify the abuse of IT and appropriate disciplinary actions for abuse; - security of cargo related documents; - signature and stamp policies; - deadlines for processing of documents; - special control for emergency/last minute shipment information (WCO SAFE Framework of Standards, C-TPAT, AEO Program, STAR initiatives, STP, BASC, ISO Standards).
7	Cooperation with authorities	<ul style="list-style-type: none"> - ISSC; - CSR; - records of activities; - provision of information about last 10 calls before entering to the port not less than 24 hours before expected entry; - CSO; - SSP (ISPS Code), - submission of information prior entering into EU port 24 hours in advance (*for all vessels entering EU countries) (EU Regulation No 725/2004), - submission of cargo manifest to US Customs 24 hours before cargo loading (*for all cargo bound to US) (AMR); - submission of Vessel Stow Plan and Container Status Message (*for all cargo bound to US) 10+2 Rule; - submission of Notice of Arrival to US ports 96 hours before arriving (*for all vessels entering US ports) (ANOA); - submission of ESM to EU ports 24 hours before cargo loading (*for all goods that are arrived to EU countries, Norway, Switzerland) (EU 24HR), - submission of cargo manifest to China Customs 24 hours before cargo loading (* for cargo bound to China), - submission of cargo manifest to Canada Customs 24 hours before cargo loading (* for cargo bound to Canada), - submission of cargo related information to Mexico Customs 24 hours before cargo loading (* for cargo bound to Mexico), - submission of Notification of Arrival to MPA (*for all vessels entering Singapore port). 	<ul style="list-style-type: none"> - details of the links with relevant authorities and the necessary communication systems; - continuing mutual exchange of information with authorities; - procedures for reporting to relevant authorities of any suspicious incidents, cargo, cargo documentation or requests for information (WCO SAFE Framework of Standards, AEO Program, BASC).

8	Security of business partners		<ul style="list-style-type: none"> - extensive exchange of information with trading partners for enhanced security coordination and cooperation; - mutual supply chain security policy; - security education, training and awareness of and by trading partners; - procedures for screening and selection of business partners; - procedures to monitor and review business partners' compliance to security requirements; - business partners' participation in supply chain security programmes administrated by foreign Customs; - mutual security agreements with trading partners (WCO SAFE Framework of Standards, C-TPAT, AEO Program, STAR initiatives, STP).
9	Crisis management and incident recovery	<ul style="list-style-type: none"> - security levels, - SSO; - SSP (ISPS Code). 	<ul style="list-style-type: none"> - contingency plans for emergency security situations and for disaster or terrorist incident recovery; - procedures for identification of potential risks and responses to security incidents and emergency situations; - development of crisis management rooms; - periodic training on crisis management; - incident tracking and information communication; - investigation capability and follow-up; - analysis of causes of crisis; - development of a BCP (WCO SAFE Framework of Standards, AEO Program, STAR initiatives, STP, ISO Standards).
10	Security assessment, response and improvement	<ul style="list-style-type: none"> - SSA; - SSP; - CSO; - SSO (ISPS Code). 	<ul style="list-style-type: none"> - integrity and adequacy of the SMS; - potential areas for improvement of the SMS; - audits and evaluation of compliance with appropriate legal requirements; - self-assessment procedures and identification of responsible parties; - follow-up actions from previous security reviews (WCO SAFE Framework of Standards, AEO Program, STAR initiatives, C-TPAT, ISO Standards).

2.2.2.2. Current Issues with Existing Maritime Security Requirements

As Table 2.2 shows, the maritime security requirements for shipping companies are divided into compulsory and voluntary classifications. While only the former are mandatory for implementation, it is strongly recommended to take into consideration the latter. Some authors believed that, although requirements of voluntary security programmes are not mandatory, noncompliance often has a negative effect on the business of shipping companies (Banomyong, 2005; Gutierrez and Hintsa, 2006; Metaparti, 2010; Rice and Spayd, 2005). For example, Banomyong (2005, p. 10) believed that “the security recommendations [of C-TPAT] will eventually become the actual requirements”. And Gutierrez and Hintsa (2006) had an opinion that compliance with voluntary security programmes has become a minimum requirement for participating in international trade. Therefore, it is important to consider both compulsory and voluntary security requirements when managing security in shipping companies.

The classification made in Section 2.2.2.1 shows the variety of existing maritime security requirements for shipping companies. This variety brings a lot of difficulties to businesses in the shipping industry in the way of their implementation. The most discussed problem is the overlapping and inconsistencies between the requirements imposed by different regulatory documents (Acciaro and Serra, 2013; Bryant, 2009; Hintsa et al., 2009; Sarathy, 2006; Thibault, et al., 2006; Yang, 2010; Papa, 2013). Gould et al. (2010, p. 297) believed that “one of the problems is that there is no single overarching framework for security programmes, and the industry faces overlapping protocols and regulations.”

For example, the ISPS Code requires vessels to submit ship security information prior to entering the port (Pallis, 2006). Similar requirements are found in the EU (EU Regulation on enhancing Ship and Port Facility Security), the US (ANOA) and Singapore regulations (DHS, 2003; EU, 2004; MPA). Besides, the requirement to submit cargo related information 24 hours before the cargo is loaded in a foreign port is contained in regulations of different countries, such as EU 24HR, US AMR, China 24HR, Canada 24HR, Mexico 24HR (CBSA, 2004; China Customs, 2008; DoT, 2002; EU, 2011; MCA, 2008). Even though the content of

these requirements is very similar, the method of submission, required information and necessary hardware and software may vary significantly. For example, Yang (2010, p. 717) found out that the problem related to the extension of the 24-h rule to Canada and China was often recorded by questionnaire respondents: “the lack of uniformity among security initiatives and security transmission systems hinders transmission operations.” Figure 2.1 shows the similar security requirements imposed by different regulations.

Figure 2.1 Similarities between compulsory maritime security requirements for shipping companies

Moreover, a majority of voluntary requirements are simultaneously found in different sources, like WCO SAFE Framework of Standards and AEO Program, C-TPAT, STAR Initiatives, BASC, STP, ISO Standards and others. This similarity between security requirements may benefit shipping companies, because compliance with one of the programs may sometimes be considered as a partial participation in another similar program, since some of the requirements have already been implemented. However, Gutierrez and Hints (2006, p. 10) believed that “it is not possible to say that a company that is certified by one program will have the requisites to be certified by another”. Although some specific requirements from different sources are quite similar to each other, the documents and programs themselves are significantly different in the process and conditions of implementation. Gutierrez and Hints (2006, p. 10) commented:

While some provide a detailed list of security standards that must be implemented in order to become security compliant, others just mention the security conditions that should be achieved, leaving room for different interpretations on how to implement them.

Hence, the need for unification among existing common standards and maritime regulations, for example, by a mutual recognition concept, is widely discussed in the literature (Voort et al., 2002; Stasinopoulos, 2003; Mikuriya, 2007; Pallis and Vaggelas, 2008; Aigner, 2010; Gould et al., 2010; Metaparti, 2010; Altemöller, 2011; Ireland, 2011; Papa, 2013). Widdowson and Holloway (2009, p. 32) believed that “there is a strong demand for standardization, harmonization and mutual (cross-border) recognition”. However, only a few studies have been conducted to compare security requirements imposed by different regulations. For example, Gutierrez and Hintsä (2006), in their research, combined security measures found in different voluntary supply chain security programs. Similarly, this thesis provides a comprehensive list of compulsory and voluntary security requirements for shipping companies, which are most often met in different regulations. These requirements are shown in Table 2.3.

Table 2.3 Compulsory and voluntary maritime security requirements for shipping companies

Compulsory requirements	Voluntary requirements for shipping companies, most often met in various voluntary security programmes
<ul style="list-style-type: none"> - develop SSP; - install SSAS and AIS; - display SIN; - ensure routing checking of cargo (ISPS Code); - appoint CSO, SSO; - carry out training and drills (ISPS Code); - ensure SID is held by every seafarer (SID Convention); - keep records of activities and CSR; - obtain ISSC; - assure necessary security level of ship (ISPS Code); - provide ship security information prior entering port (ISPS Code, EU Regulation No 725/2004, US ANOA, Singapore MPA); - submit cargo related information 24 hours before cargo loading (US AMR, EU 24HR, China 24HR, Canada 24HR, Mexico 24HR); - submit VSP and CSM prior arrival to US port (10+2 Rule); - undertake SSA (ISPS Code); 	<ul style="list-style-type: none"> - CCTV, - access control; - identification of employees, visitors, vendors; - inspection of persons and packages; - written procedure for sealing of cargo; - strict procedure for inspection of full and empty containers; - constant control all cargo during shipping processes; - screening of current and prospected employees; - procedures for hiring, induction, retaining and termination of employees; - organizational roles and responsibilities; - awareness of the security management policy; - periodic training on crisis management; - continuing mutual exchange of information with authorities; - procedures for reporting to relevant authorities of any incidents; - security management documentation system; - procedures for controlling all documents, data and information; - mutual supply chain security policy with business partners; - procedures for screening and selection of business partners; - contingency plans; - analysis of causes of crisis; - BCP; - integrity and adequacy of the SMS; - audits and evaluation of compliance with appropriate legal requirements; - self-assessment procedures.

2.2.2.3. Implementation of Maritime Security Requirements

However, it is possible that not all of the requirements in Table 2.3 are practically implemented, often because of the lack of resources. In this respect, not many studies have been conducted to examine the implementation of maritime security requirements. Gutiérrez et al. (2007) investigated which security measures were commonly implemented by BASC member companies, as well as the cost and effectiveness of their implementation. It was found that the most often implemented voluntary security measures refer to human resource management and the most effective measures are those of facility management and information management. While Gutiérrez et al. (2007) studied the effectiveness only with respect to security improvement, Voss et al. (2009) and Thai (2007) also looked at some other aspects of organizational performance. Besides, Tsai (2014), in his paper, was studying the implementation of security measures on board ship. Additionally, there are several studies conducted by the US Government Accountability Office (2008a, 2008b, 2008c), which examined the effectiveness of different security regulations, such as the US C-TPAT. Since shipping companies have to implement requirements imposed by different regulations, it is necessary to study these requirements together. Additionally, it is important to know how effective security requirements are because the lack of knowledge on this topic may lead to the unwillingness of shipping companies to implement these requirements (Altemöller, 2011; Thibault, et al., 2006; Voss, et al., 2009; Yang, 2010). Some authors also believed that the effectiveness of security requirements may vary from one company to another, and thus, the approach to security management chosen by various shipping companies may result in different consequences (Gutiérrez, et al., 2007; Thai, 2007). This argument leads to another very important question on how to manage security effectively in shipping companies.

2.3. Effective Maritime Security Management in Shipping Companies

As discussed in Section 2.2.2.2, the diversity of maritime security regulations poses a very important problem for shipping companies - how to meet and maintain

the requirements while not jeopardizing other organizational performance, in other words, how to manage maritime security effectively. Thus, the topic of maritime security management is widely discussed in related academic and industrial publications. However, maritime security is a comparatively young topic on the international maritime agenda. The majority of the security regulations for shipping companies have been introduced within the last ten years. That is the reason why not many papers studying the concept of *maritime security management* have been found. To widen the literature review for this research question, studies on *supply chain security management* and *transportation security management* have also been included. This section is organized as follows. Firstly, the management approaches applicable for security management as well as maritime security management frameworks and models are reviewed. Then the existing problems of maritime security management in shipping companies are identified. Finally, based on the discussed approaches and the problems, a list of essential criteria for the EMSMM in shipping companies is presented.

2.3.1. Definition of Maritime Security Management

Among the reviewed literature, not many sources contain the definition of security management. For example, the ISO, in its ‘Specification for security management systems for the supply chain’, provided the following definition of security management: “systematic and coordinated activities and practices through which an organization optimally manages its risks, and the associated potential threats and impacts therefrom” (ISO, 2007, p. 2). Closs and McGarrell (2004, p. 8) defined supply chain security management as follows:

The application of policies, procedures, and technology to protect supply chain assets (product, facilities, equipment, information, and personnel) from theft, damage, or terrorism, and to prevent the introduction of unauthorized contraband, people, or weapons of mass destruction into the supply chain.

Whereas, Hintsa, et al. (2009, p. 2) explained supply chain security management as “enhancing and embedding the traditional security management aspects into holistic management of integrated supply chains.” Additionally, while discussing supply

chain security management, Gutiérrez (2007, p. 23) indicated that “understanding the mechanisms behind the suggested security measures of these programs and implementing them in an effective way is one of the biggest challenges for companies.”

Based on the provided statements, for the purpose of this research, maritime security management is defined as *an essential and integrated part of the overall company management, focusing on the coordination of the shipping company's activities on the implementation of compulsory and voluntary security requirements, as well as other security related activities, for the purpose of managing security related risks inside and outside the company.*

2.3.2. Existing Approaches and Models of Maritime Security Management

Several attempts have been made by international organizations, national governments, industry professionals and researchers to help shipping companies to manage maritime security. Firstly, some of the voluntary security programs, such as SAFE Framework of Standards, ISO Standards, STAR Initiatives, STP, BASC Initiatives, etc., provide guidance for security management in shipping companies and other supply chain companies. Secondly, significant contribution has been done by researchers in this area. Some of them described management approaches and tactics that may be useful in the supply chain or maritime security management. Others proposed frameworks, models and systems of security management in shipping and supply chain organizations.

It was observed that, when discussing maritime security management, authors most often mentioned such approaches as risk management (RM), quality management (QM) or total quality management (TQM), business continuity management (BCM), disaster management (DM), crisis management (CM) and security management (SM) or total security management (TSM).

RM is a common management approach used for managing security in companies. Thai (2009, p. 150) defined it as follows:

Risk management 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 description or application of this approach was found in the studies of Bichou (2004), UNCTAD (2006), Thai and Grewal (2007), Rice and Tenney (2007), Talley (2008), Williams, et al. (2008), Autry and Bobbitt (2008), Bernard (2009), Thai (2009), Christopher (2009) and Gould, et al. (2010). A risk-based methodology generally consists of a five-step process: hazards identification, risk assessment, risk management with alternative options, cost-benefit analysis (CBA) and decision making. The two basic measures in a risk model are the probability of an event occurring, and its consequences. Thus, standard risk prevention strategies aim either at reducing the probability of an incident (pre-accident intervention) or at minimising the probability of fatalities if the accident occurs (post-accident intervention) (Thai, 2009; UNCTAD, 2006).

According to Gutiérrez (2007, p. 10), “in the context of supply chain, two main approaches [to RM] have been identified: Supply chain Vulnerability Management and Disaster Management (DM)”. The former focuses on the factors of supply chain which initiate risks and increase the possibility of their occurrence, the latter focuses on the consequences of the external threats (Gutiérrez, 2007). Therefore, these two main approaches of RM shall be applicable in shipping companies to minimize the probability of security incident and to reduce any possible undesirable consequences. Moreover, Williams, et al. (2008), based on the framework of Juttner et al. (2003), presented a model of supply chain RM, which consists of Risk sources, Risk drivers, Risk mitigation strategies and Risk outcomes. Additionally, Rice and Tenney (2007) proposed the maturity levels of supply chain RM. They are based on the level of compliance of the supply chain organization with security requirements: pre-compliant, compliant, secure and resilient. A similar classification of security levels was proposed by Rice and Caniato (2003b). These maturity levels may be practically implemented by shipping companies for self-assessment.

Another frequently discussed approach to security management in shipping and supply chain organizations is QM or TQM (Bichou, et al., 2007; Frankel, 1993;

Gould, et al., 2010; Hintsa, et al., 2009; Lee and Whang, 2005; Sarathy, 2006; Talley, 2008; Thai, 2009; Thai and Grewal, 2007; UNCTAD, 2006; Urciuoli, et al., 2010; Williams, et al., 2008). In the maritime related literature, QM is defined as an improvement of “process performance continuously by placing shippers’ interests at the forefront of all efforts [...], while still operating in a cost-effective manner” (Bichou, et al., 2007, p. 11). QM is based on the eight main principles, some of which can be useful in the security management concept, such as security prevention from the source, process control and management for security purpose, total organizational focus in security management, and continuous security improvement (ISO, 2000, 2005; Lee and Whang, 2005; Thai, 2009).

In the maritime security related literature, QM is applicable in different ways. Several authors proposed applying Six Sigma cycle for security management (Lee and Whang, 2005; Williams, et al., 2008). Thai (2008) put Plan-Do-Check-Act (PDCA) cycle as a concept of continuous security improvement principle, as shown in Figure 2.2. Meanwhile, Bichou, et al. (2007) introduced the QM-based framework for implementing a regulatory maritime security program, containing ten steps: Management Commitment, Maritime Security Improvement Team, Maritime Security Performance Standards, Awareness of Maritime Security, Managers' and Supervisors' Training, Goal Setting for Maritime Security, Error Cause Removal, Corrective Actions, Recognition and Reward, and Continuous Improvement. Accordingly, the PDCA cycle shows the general idea of continuous security improvement, whereas the framework can be used as a part of guidance for the security management, since it provides the detailed steps. Moreover, these recommended approaches are essential for effective security management, because they amend the QM principles to be applicable for security management, and they also connect and combine the QM and RM approaches.

Figure 2.2 The Continuous Security Improvement (CSI) cycle

Source: Thai (2009, p. 150)

BCM is another often discussed approach in the literature on maritime security management (Autry and Bobbitt, 2008; Gould, et al., 2010; Gutiérrez, 2007; Nevrous, 2010; Rice and Caniato, 2003a; Thai, 2009; Williams, et al., 2008). Hiles and Barnes (2001) in Gould, et al. (2010, p. 296) defined BCM as follows:

The development of strategies, plans and actions which provide protection or alternative modes of operation for those activities or business processes which, if they were to be interrupted, might otherwise bring about a seriously damaging or potentially fatal loss to the enterprise.

It is argued that BCM is more important when the so called ‘rare events’ occur, such as terrorist attacks, computer network virus attacks or natural disaster, rather than smaller security incidents (Nevrous, 2010). Thus, it is designing the system to “fail smartly”, by preparing backups, training people and making security and resilience a part of the company’s culture (Rice and Caniato, 2003a). BCM should also include activities such as the process flow, documentation, hierarchy, backup communication, checklists, maps, and agreements for critical suppliers, etc. (Williams, et al., 2008). BCM is usually based on crisis management (CM), disaster recovery or disaster management (DM), business recovery and contingency planning (Norman and Jansson (2004) in Gould, et al. (2010).

CM represents an organizational response capacity to deal with incidents, it usually includes four steps: prevention, preparation, response and recovery (Autry and Bobbitt, 2008; Barnes and Oloruntoba, 2005). DM was defined in Gutiérrez (2007, p. 13) as the way of:

reducing external supply chain risks by focusing on the consequences of the disruption implies dealing with three main objectives: i) failing smartly, ii)

continuing operations in the best possible way during the disruption and iii) recovering back to normal situation in a prompt way and reducing as much as possible the negative sequels.

This approach is based on the development of redundancy, flexibility, supply chain knowledge and culture (Gutiérrez, 2007). A similar approach is a disruption management which has two key phases, such as “discovery” (of the event) and “recovery” (from the event) (Macdonald and Corsi, 2013).

Moreover, Business Continuity Planning (BCP) is an essential part of BCM. Rice and Caniato (2003a, p. 27) defined it as “developing plans to be resilient – that is, to be prepared to respond to and restore operations after an unexpected, major disruption occurs.” The authors argued that BCP might also help companies to decide on the levels of security and resilience, to choose the necessary measures for different targets, to prepare backup plans, and so forth. Zsidisin et al. (2005) in Autry and Bobbitt (2008) proposed four steps of BCP; they are awareness creation, prevention, remediation and knowledge management.

Additionally, some authors associated BCM with a layered approach to security management. They believed that this approach helps companies to build the redundancy, which means to guard all levels of the system from the security breaches occurring in one of them (Bichou et al., 2014; Rice and Caniato, 2003a; Sarathy, 2006; Urciuoli, et al., 2010; Williams, et al., 2008). This approach usually includes actions such as an assessment of supplier security and resilience, development of the information systems with alternative communication system backup, emergency plans for response to disruption, and etc. (Rice and Caniato, 2003a).

It can be concluded that BCM is closely related to RM and QM. One of the purposes of RM is to reduce the consequences of the security incident. Similarly, BCM aims to minimize the possible negative consequences by preparing to deal with them and therefore continue operations. Moreover, BCM is based on some principles of QM, such as the creation of security culture, security awareness and training of all employees, security prevention from the source. Therefore, to develop an effective security management model, it is necessary to view all these management approaches as a single strategy, where all elements are derived from

the principles of RM, QM and BCM. Thus, some authors introduced the concept of TSM. Ritter et al. (2007, p. 17) in Williams et al. (2008, p. 266) defined this approach as “the business practice of developing and implementing comprehensive risk management and security best practices for a firm’s entire value chain.” It is based on a continuous improvement, TQM, and six sigma philosophies, and includes activities such as the development of the internal policies and procedures in terms of preparedness for disruptive events such as terrorism, political upheaval, natural disasters, and significant accidents; and evaluation of business partners and relationships (Williams, et al., 2008). Table 2.4 provides a summary of specific management approaches of security management in the existing literature.

Table 2.4 Management approaches of security management in existing literature

Management Approach	Source
RM	Thai and Grewal, (2007); Rice and Tenney, (2007); Talley, (2008); Williams, et al., (2008); Autry and Bobbitt, (2008); Bernard, (2009); Thai, (2009); Christopher, (2009); Gould, et al., (2010).
QM/TQM	Bichou, et al., (2007); Thai and Grewal, (2007); Talley, (2008); Thai (2008); Williams, et al., (2008); Hintsu, et al., (2009); Thai, (2009); Gould, et al., (2010); Urciuoli, et al., (2010); Thai (2013).
BCM	Gutiérrez, (2007); Autry and Bobbitt, (2008); Williams, et al., (2008); Thai, (2009); Gould, et al., (2010); Nevrous, (2010).
DM	Barnes and Oloruntoba, (2005); Autry and Bobbitt, 2008; Macdonald and Corsi, 2013
CM	Gutiérrez, (2007).
Layered Approach	Bichou et al., 2014; Williams, et al., (2008); Urciuoli, et al., (2010).
TSM	Ritter et al. (2007) in Williams et al. (2008);

The reviewed approaches have been variously applied by authors who proposed models, systems and frameworks for security management. In a study by Gutiérrez (2007), the Supply Chain Security Management Model (SCSMM) was developed based on the principles of RM, TQM and BCP. The proposed model is expected to help supply chain companies achieve a balance between security, resilience and efficiency. The author distinguished between supply chain management and

security chain management. Supply chain consisted of cargo, information, facilities, human resources, and business partners. Security chain combined information flow and security measures of three categories: protection, monitoring and detection, and reaction. Moreover, the model included four supply chain factors, which are visibility, responsibility network, balance of weak links, and capacity configuration, and two security chain factors, namely synchronization of security functions and security bullwhip effect. To develop the framework for supply chain security management, Closs et al. (2008) combined principles of TQM and DM. The authors listed ten competences essential for the supply chain security management, namely Process Strategy; Process Management; Infrastructure Management; Communication Management; Management Technology; Process Technology; Metrics; Relationship Management; Service Provider Collaboration Management; and Public Interface Management. These components were derived from the principles of TQM and DM.

In the context of shipping companies, there are only a few studies found focusing on security management. Specifically, the conceptual model of effective maritime security proposed by Thai (2009), consists of 13 dimensions, including 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 Security incident handling and response. These dimensions and their associated critical success factors were derived based on a combination of principles of RM, QM and BCM. Moreover, Thai and Grewal (2007) developed the Maritime Security Management System (MSMS). This system combines six key elements, namely activities, main players, organizational relationships, security dimensions, security elements and criteria. The main security dimensions include security awareness education and training, access control, physical security, procedural security, personnel security, and information security. Besides, the MSMS proposes the security criteria for maritime security management, such as holistic approach, constant reviewing, and security as part of a wider safety

management system, adequate guidelines, integration of RM, QM, and environmental management and other safety systems, etc. Among others, the proposed system is the most comprehensive framework for security management in shipping companies.

The reviewed approaches to security management as well as systems, models and frameworks provide an essential background for the effective management of maritime security in shipping companies. The key strengths of these studies are that the authors used a combination of different management approaches, such as RM, TQM, BCM, etc. However, some limitations of the proposed models and systems have been found. Both the MSMS and the SCSMM provide a very comprehensive and detailed framework for security management in the companies. However, none of them is clearly linked to the list of security requirements. Even though the SCSMM is based on five categories of voluntary security measures, it does not consider the compulsory requirements for supply chain organizations. Moreover, the SCSMM is a very wide model for security management in supply chain companies, however it does not consider the features of different types of businesses in the supply chain. From this point of view, the MSMS is more focused on shipping companies. Besides that, none of the discussed models and systems considers the impacts of security management on organizational performance. Even though the SCSMM aims to achieve the balance between security, efficiency and resilience, the author does not link it to any specific organizational performance. Finally, none of the reviewed frameworks provides guidance for managers with regards to the practical implementation in the companies. Thus, to fill the existing gaps, the lessons from existing literature should be combined to develop an effective maritime security management model.

2.3.3. Problems of Maritime Security Management in Shipping Companies

As argued previously, one of the most discussed problems of managing security in shipping companies is overlapping and inconsistency between the requirements imposed by different regulatory documents (Acciaro and Serra, 2013; Bryant, 2009; Hintsa, et al., 2009; Papa, 2013; Sarathy, 2006; Thibault, et al., 2006; Yang, 2010).

Gould et al. (2010, p. 297) believed that “there is no single overarching framework for security programmes, and the industry faces overlapping protocols and regulations.” For example, some compulsory requirements, such as the submission of ship security information prior to entering the port and submission of cargo related information 24 hours before loading, are met in regulations of different countries. Even though the content of these requirements is very similar, the method of submission, required information and necessary hardware and software may vary significantly (Yang, 2010). Moreover, voluntary programs, such as the WCO SAFE Framework of Standards and AEO Program, C-TPAT, STAR Initiatives, BASC, STP, ISO Standards and others, often contain very similar requirements. However, compliance with the requirements of one of the programs does not automatically lead to certification for others (Gutierrez and Hintsa, 2006). Thus, the question on the necessity of unification of the existing common standards and maritime regulations in achieving consensus on maritime security issues is widely discussed now (Metaparti, 2010; Papa, 2013; Pallis and Vaggelas, 2008; Stasinopoulos, 2003; Voort, et al., 2002).

Some authors were also concerned about the breaches in maritime security regulations. “The security initiatives that are in place cover international shipping, while shippers and carriers see a need for security improvements in domestic shipping, as well” (Gould, et al., 2010, p. 297). Thai and Grewal (2007) suggested that while there are no legal requirements to cover these breaches, shipping companies have to manage this problem by themselves. Additionally, ‘bureaucracy’ and ‘government red tape’ were reported among observed problems (Autry and Bobbitt, 2008).

Several authors also highlighted a need for a comprehensive security management framework, as well as specific and detailed guidelines for security management (Acciaro and Serra, 2013; Closs, et al., 2008; Urciuoli, et al., 2010). Bichou (2011) commented that some security regulations, such as the ISPS Code, contain general provision on security requirements, but do not prescribe detailed and uniform instructions on how to comply with them. The lack of instructions and guidelines brought managers a lot of questions such as how to allocate resources and invest wisely in security, which security initiatives to comply with, and whom

to partner with, for the purpose of achieving a good balance between implementation and impacts (Gould, et al., 2010; Hintsa, et al., 2009; Papa, 2013; Sarathy, 2006; Williams, et al., 2008). Furthermore, the situation could be aggravated by difficulties in quantifying impacts of the implementation of security initiatives on organizational performance of shipping companies. Voss, et al. (2009, p. 10) commented:

It is difficult to justify security related investment because firms primarily focus on direct expenses and not collateral benefits... Additionally, some managers do not perceive their firm to be vulnerable to security threats because their firm handles less critical commodities.

Thus, managers simply do not understand how the introduced security measures may help their organizations to prevent and recover from terrorist attack (Thibault, et al., 2006; Yang, 2010), since very limited information about the attacks was available (Eyefortransport, 2002; Urciuoli, et al., 2010). Generally, the discussed problems might be partly solved or mitigated by implementing an effective management approach or management model in a shipping company.

2.3.4. Essential Criteria for the EMSMM in Shipping Companies

An effective model of security management in shipping companies should satisfy several essential criteria. In this thesis, a list of essential criteria for the EMSMM was derived. As Figure 2.3 shows, the criteria were derived based on the management approaches and proposed security management models and systems, reviewed in Section 2.3.2, as well as with consideration of the problems discussed in Section 2.3.3. The management model, satisfying the essential criteria, is expected to help achieve its main purpose – to find a balance between security, resilience and efficiency.

Figure 2.3 Deriving essential criteria for the EMSMM

The list contains the following seven criteria:

1. *The EMSMM is easily applicable in practice and provides guidance for implementation.* Some academic and industrial publications indicated that maritime security regulations are often considered by shipping companies as vague and not very precise. Even though managers in companies “are greatly concerned about security, many are still unsure about how to move forward with a comprehensive security plan” (Closs, et al., 2008, p. 40). Thus, to help managers to implement the model in shipping companies, it is necessary to develop a clear understanding and transparent model, containing necessary guidelines for implementation. For example, Gutiérrez (2007) used the proposed model to describe the supply chain security management system of the two case study companies, whereas, Closs, et al. (2008), in their security management framework, provided examples of the security measures for each competence of the framework. Hence it is suggested that the EMSMM should not only contain the model of security management, but also provide the guidance for its implementation.

2. *The EMSMM helps managers to implement compulsory and voluntary maritime security requirements.* One of the purposes of the effective security management is to implement the maritime security requirements to achieve the necessary security level, without jeopardizing other organizational performance of shipping companies (Thai, 2009). Therefore, when developing the EMSMM, it is

necessary to consider the compulsory and voluntary maritime security requirements. For example, Gutiérrez (2007) based the proposed model of supply chain security management on five categories of voluntary security measures, however, the compulsory requirements were not considered in the model.

3. *The EMSMM is developed specifically for shipping companies.* Several models or frameworks have been developed for security management in the supply chain. Although shipping companies are important elements of the supply chain, they have their own features that should be considered when developing the EMSMM. A significant contribution here has been made by Thai and Grewal (2007) who proposed the maritime security management system whose key elements reflected the features of shipping companies.

4. *The EMSMM aims to achieve the balance between security, efficiency and resilience.* Many studies discussed the trade-offs between security and resilience (Rice and Caniato, 2003a, 2003b; Williams et al., 2009), between security and efficiency (Burns, 2013; Gould, et al., 2010; Hints, et al., 2009; Williams, et al., 2008), and sometimes between efficiency and resilience (Sheffi, 2001). However, just a few researchers discussed the necessity to achieve a balance between all three components: security, efficiency and resilience. A comprehensive literature review on this question has been conducted by Gutiérrez (2007). The author noted the importance of distinguishing between security, resilience and efficiency:

A secure system is one with all the required mechanisms to prevent a disruption, a resilient system is one which fails smartly and reacts adequately to disruption and an efficient system is one that produces the maximum value with the least possible cost (p.27).

To manage trade-offs between security and resilience, BCM and the layered approach are often proposed in the literature (Rice and Caniato, 2003a, 2003b; Sarathy, 2006; Sheffi, 2001). The balance between security and efficiency is often managed by applying the TQM approach, as well as visibility, monitoring and control (Gould, et al., 2010; Gutiérrez, 2007; Williams, et al., 2008). Gutiérrez (2007) proposed the following components for managing trade-offs between resilience and efficiency: risk consideration, visibility, clear performance

requirements, and business partners' requirements. All the reviewed recommendations and approaches are essential for the EMSMM.

5. *The EMSMM links security management and its impacts on organizational performance.* One of the problems of the existing security management models or frameworks is that they do not evaluate how their application impacts organizational performance. However, it is important to know the results of the chosen management approach, to decide if necessary changes are required. Therefore, the effective security management model should include performance measurement.

6. *The EMSMM is based on a holistic approach to security management.* Many authors argue that security management needs to become an essential and integrated part of corporate strategy (Gutiérrez, 2007; Sarathy, 2006; Williams, et al., 2008). "Since security is a problem for the whole organization, it is simply no longer effective or acceptable to manage it from the security department" (Thai, 2009, p. 149). Researchers suggested that security should become integral with other activities and considered in other departments of the organization (Metaparti, 2010; Sarathy, 2006). They proposed to 'create a security culture' (Gould, et al., 2010) in supply chain organizations by bringing together the organization's security and supply chain functions and by enhancing the organizational leadership (Rice and Caniato, 2003a). Moreover, a holistic EMSMM should involve both micro- and macro-levels of the maritime industry (Thai and Grewal, 2007). Since shipping companies are elements of the whole supply chain, the security management cannot be limited by the company's framework. Therefore, the EMSMM should facilitate a holistic approach to security management and widen beyond the organization's framework.

7. *Finally, the EMSMM is easily adopted by different shipping organizations.* Not every shipping company is required to have the same security level. It may depend on the size and type of the company, activities and other features. Moreover, the initial level of security compliance may vary in different companies (Rice and Tenney, 2007; Rice and Caniato, 2003b). Therefore, it is argued that the EMSMM should be flexible and provide managers some freedom in implementation. For this purpose, the self-assessment approach plays an important role.

The listed criteria can be summarized and become requirements for the proposed model. In brief, the EMSMM should be based on the balance of security, efficiency and resilience. For this purpose, the holistic approach should be applied to make security a part of all organizational processes, and organizational performance needs to be evaluated and linked to security management activities. Additionally, the EMSMM should be flexible and easy for implementation. To satisfy this requirement, a detailed guidance needs to be developed with consideration of the features of shipping companies. Finally, since the compliance with security regulations is a mandatory condition for the companies, the model should promote the effective implementation of compulsory and voluntary security requirements. However, the majority of the maritime security management models, frameworks or systems, found in the related literature, do not satisfy all of the essential criteria. Table 2.5 lists the criteria and highlights the corresponding models and frameworks that have addressed these criteria in the literature.

Table 2.5 Essential criteria for the EMSMM in shipping companies

Essential Criteria	Model or system satisfying the criteria
1. The EMSMM is easily applicable in practice and provides guidance for implementation.	Supply Chain Security Management Model (SCSMM) in Gutiérrez (2007); Framework for Supply Chain Security Management (FSCSM) in Closs, et al. (2008)
2. The EMSMM helps managers to implement compulsory and voluntary maritime security requirements.	SCSMM in Gutiérrez (2007)
3. The EMSMM is developed specifically for shipping companies.	Maritime Security Management System (MSMS) in Thai and Grewal (2007)
4. The EMSMM aims to achieve the balance between security, efficiency and resilience.	SCSMM in 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 in Thai and Grewal (2007); Effective Maritime Security Model (EMSM) in Thai (2009)
7. The EMSMM is easily adopted by different shipping companies.	MSMS in Thai and Grewal (2007); EMSM in Thai (2009)

2.4. The Link between Maritime Security and Organizational Performance of Shipping Companies

The main purpose of the discussed initiatives is to enhance maritime security in shipping companies. However, besides the expected benefits, the implementation of maritime security initiatives often has negative impacts on organizational performance of the companies. The misunderstanding of benefits, as well as achievement of negative results may jeopardize the implementation of security regulations in shipping companies (Peleg-Gillai et al., 2006; Thibault, et al., 2006; Voss, et al., 2009; Yang, 2010). Even though, some authors have already addressed the problem of analysing the impacts of maritime security accidents (Fu et al., 2010), however “impacts of maritime security still remain under-researched and fragmented” (Bichou et al., 2014, p. 3). Thus, a clear vision of the impacts of maritime security initiatives on organizational performance of shipping companies is necessary to enhance the awareness within shipping industry on the necessity and effectiveness of these initiatives.

This section aims to review literature on changes in organizational performance of shipping companies caused by security management. Firstly, the review of the impacts is provided based on several categorizations, such as positive and negative impacts, short-term and long-term, proposed and reported. Secondly, the definition of organizational performance is provided. The general concept of organizational performance and its categories and indicators is then explained, followed by a discussion on impacts of maritime security initiatives on organizational performance of shipping companies. Finally, the methods for objective measurement of the impacts are reviewed.

2.4.1. Impacts of Implementation of Maritime Security Requirements

Scientific and industry publications provide broad information on how implementation of security requirements and management of maritime security in shipping companies affected or may affect their performance. This section classifies

the available information based on several criteria of impacts, such as positive and negative, proposed and reported, and short-term and long-term impacts.

Since the main purpose of maritime security requirements is to improve security, some regulations or government documents provide benefits that shipping companies can enjoy after implementation of specific security measures (APEC, 2002; BASC, 2002; CBP, 2001; ISO, 2007; Singapore Customs, 2011; WCO, 2007). Besides, there are many papers focusing mostly on positive impacts (Crutch, 2006; Fletcher, 2007; Gutiérrez, et al., 2007; Peleg-Gillai, et al., 2006; Thai, 2007). However, several papers covering negative impacts were also found (Banomyong, 2005; Bichou, 2008; Thibault, et al., 2006; Urciuoli, et al., 2010; Yang, 2010).

For example, security improvement in shipping companies were often discussed in literature and proven by existing data. A decline in the number of accidents was mentioned as one of the most important improvements (APEC, 2002; Eyefortransport, 2002). The changes such as a reduction in the number of cargo theft and its consequences, reduction in smuggling, tampering and damages, quicker recovery from accidents and better problem response (Gutiérrez, et al., 2007; Peleg-Gillai, et al., 2006; Voort, et al., 2002), a reduction in frequency of person to be stowaway (see Figure 2.4) and a decline in number of attacks against ships (see Figures 1.1 and 1.2) have been observed within first several years after the initiatives started to be implemented (Bichou, 2008; Timlen, 2007). Additionally, security awareness in shipping companies has been significantly improved (Thai, 2007; Thibault, et al., 2006). Thibault, et al. (2006, p. 10) indicated that “new security training requirements have made workers at maritime facilities more willing to address or report security concerns”. Besides, changes in efficiency, reliability, flexibility and visibility were also found in several sources, however just a few of them provided reliable information (ISO, 2007; Urciuoli et al., 2010; Yang, 2010). The positive impacts on governing were expressed in the improvement in document processing, cargo handling, manpower utilization, inventory management, data management, and better use of IT (ISO, 2007; Peleg-Gillai, et al., 2006; Thai, 2007; Thibault, et al., 2006).

Figure 2.4 Reported incidents involving stowaways from 2002 to 2009

Source: International Maritime Organization (various years)

The requirements of some regulations for shipping companies to share security related information with government and business partners (APEC, 2002; CBP, 2001, 2002, 2009; DoT, 2002; EU, 1994, 2007, 2011; IMO, 2002; ISO, 2007; WCO, 2007) were considered as negative, since they may increase the risk of disclosure of sensitive information (APEC, 2002; Yang, 2010). However, some authors believed that cooperation with business partners and government helps to maintain a higher level of security, not only inside shipping companies, but also in the whole supply chain (Thibault, et al., 2006). Additionally, some personnel related problems, such as the need for extra staff and security training, additional workload and issues related to shore leave of seafarers, were found among the negative impacts of implementation of maritime security initiatives in the shipping companies (Goulielmosa et al., 2014; Thai, 2007; Timlen, 2007; Yang, 2010).

Besides, the impacts on time performance were also indicated in the literature. After the implementation of the new security regime, the overall time of different operations and procedures increased significantly since the whole strategy of the business was changed (APEC, 2002). This was caused by the increased number of inspections, documentation overload, delays, and port congestions (Banomyong, 2005; Thai, 2007; Urciuoli, et al., 2010; Voort, et al., 2002; Yang, 2010). However, some authors indicated that time and cost of operations may be further reduced, especially in the aspect of a long-term period, due to decreased number of

inspection, priority for inspections, and the expedited processing of cargo (Banomyong, 2005; Eyefortransport, 2002; Gutiérrez, et al., 2007; Peleg-Gillai, et al., 2006; Thibault, et al., 2006; Voort, et al., 2002).

Additionally, some information was found regarding the impacts on companies' competitiveness and branding. Some authors believed that the implementation of maritime security initiatives negatively affected competitiveness and branding of shipping companies (Yang, 2010), while others had opposite opinion (Banomyong, 2005; Gutiérrez, et al., 2007; Thai, 2007). For example, Thibault, et al. (2006, p. 11) mentioned that "there was very little evidence of switching transportation suppliers for security reasons". Besides, increased customer satisfaction was mentioned in several publications (Eyefortransport, 2002; ISO, 2007; Peleg-Gillai, et al., 2006; Thibault, et al., 2006). Some of the shipping industry practitioners indicated that "compliance with the new security requirements prevented them from losing customers due to security issues" (Thibault, et al., 2006, p. 11). However, higher security taxes passed to customers and higher security tariffs might be considered as a negative impact on customer performance (Pallis and Vaggelas, 2007; Voort, et al., 2002).

The impacts on financial performance of shipping companies are most rarely discussed in the literature. References regarding changes in revenue or profit, such as increased revenue or financial loss related to implementation of security requirements, were found only in a few sources (ISO, 2007; Thibault, et al., 2006; Yang, 2010). Besides, a significant increase in cost was also mentioned in many sources (Thai, 2007; Thibault, et al., 2006; Urciuoli, et al., 2010; Yang, 2010). The initial investments for shipping companies were huge, and even the annual amount spent for maintenance of the security regime was quite high (see Table 2.6) (APEC, 2002; Banomyong, 2005). The additional cost significantly influenced the cash flow of the companies, and for some of them even led to bankruptcy (Voort, et al., 2002). With no possibility to sustain such a big expense, some companies had to pass part of them to their customers in the form of additional cost or taxes (Eyefortransport, 2002; Thibault, et al., 2006; Voort, et al., 2002). An increase in salary for a newly required staff was another addition to the existing cost (Urciuoli, et al., 2010).

Table 2.6 BASC Certification and maintenance average cost for different turnovers (with a sample size 90)

Annual turnover	Number of companies	Average value in USD			
		Implement- tion cost	Annual maintenance cost	Maintenance/ certification cost	Certification cost/ turnover
< 50,000	4	28,625	2,888	10%	>57%
50,000 – 500,000	13	17,176	8,539	50%	3% - 34%
500,000 – 1 million	13	13,585	6,698	49%	1% - 3%
1 million – 5 million	25	61,820	15,826	26%	1% - 6%
> 5 million	35	52,742	28,484	54%	<1%
Total	90	34,790	12,487	38%	

Source: Gutiérrez, et al. (2007)

All positive and negative impacts of implementation of maritime security requirements on organizational performance of shipping companies, found in the reviewed literature, are summarised in Table 2.7. The table also indicates the sources, from which the information about the impacts was retrieved.

It can be seen from Table 2.7 that some performances, such as cost, time, competitiveness, flexibility, reliability, etc., have simultaneous positive and negative impacts on them. The reason is that the proposed classification of impacts is not comprehensive enough. It is possible to classify the impacts further based on other criteria. For instance, the same performance can be impacted positively and negatively depending on the duration of the implementation of security requirements. Similarly, it is possible that the impact was proposed as positive; however the real data shows a negative result. Discrepancies can be avoided by providing other levels of classification based on different criteria.

It is believed that impacts of the implementation of maritime security requirements on organizational performance may change with time. Therefore, in some studies, the impacts are divided into short-term and long-term, where the former usually lasts for several years, and the latter continues for decades of years (Banomyong, 2005; Bichou, 2011; Thai, 2007; Voss, et al., 2009). Moreover, most of the authors believe that short-term impacts are usually negative, whereas long-term ones are mostly positive. An example can be taken from Thai (2007, p. 339):

Table 2.7 Impacts of implementation of maritime security requirements on organizational performance of shipping companies

Positive Impacts	Source	Negative Impacts	Source
<ul style="list-style-type: none"> • increase in revenue • enhanced branding • increased competitiveness • reduce of cost: <ul style="list-style-type: none"> - reduce of insurance cost • reduce of transit time • improved efficiency • increased visibility • increased liability • improved security: <ul style="list-style-type: none"> - reduced pilferage - reduced stowaways - reduced attacks - reduction in tampering - reduction in damages - reduction in smuggling • security awareness • better cooperation btw company and gov-t • reduced number of inspection • priority for inspection • better governance: <ul style="list-style-type: none"> - better use of IT - better document processing - improved cargo handling - improved manpower utilization - improved inventory mngt - better data mngt • better problem response • quicker recovery from accidents • customers' satisfaction • higher customer service 	<p>10</p> <p>7,9,13,14,15</p> <p>2,7</p> <p>2,3,9</p> <p>3,9</p> <p>2,3,6,12,13,19</p> <p>1,10,14</p> <p>3,6,14,19</p> <p>2</p> <p>2,10,15</p> <p>1,6,7,9,12,14,19</p> <p>17</p> <p>17</p> <p>12</p> <p>9,12</p> <p>9</p> <p>13,15,16</p> <p>3,11,16</p> <p>5,6,7,8,13,14,16</p> <p>5,8,16</p> <p>1,12</p> <p>1,11,15</p> <p>10,15,16</p> <p>6,10,12</p> <p>10,12</p> <p>10</p> <p>3,6,10,12</p> <p>6,9,12</p> <p>9</p> <p>10,12</p> <p>13</p>	<ul style="list-style-type: none"> • financial loss • reputation injury • lower competitiveness • additional cost: <ul style="list-style-type: none"> - higher salary - increase insurance premiums • longer process time: <ul style="list-style-type: none"> - delays in container clearance - congestions • less reliability • less flexibility • sharing of the information with gov-t • risk of disclosure of sensitive information • need for extra staff • need for staff training • staff shore leave • extra workload • higher security taxes and tariffs • decline of late bookings 	<p>16,21</p> <p>21</p> <p>16,21</p> <p>1,2,3,11,15,16,18,21</p> <p>18</p> <p>12</p> <p>1,3,11,12,18,21</p> <p>1,4,11,12,15,19,21</p> <p>2,21</p> <p>18</p> <p>18,21</p> <p>1,20</p> <p>4,21</p> <p>15</p> <p>1,19</p> <p>17,23</p> <p>15,21</p> <p>11,16,19, 22</p> <p>3</p>

Notes: numbers in brackets indicate following publications: 1, APEC (2002); 2, Banomyong (2005); 3, Bichou (2008); 4, Bryant (2009); 5, CBP (2001); 6, Crutch (2006); 7, Eyefortransport (2002); 8, Fletcher (2007); 9, Gutiérrez et al. (2007); 10, ISO (2007); 11, OECD (2004); 12, Peleg-Gillai et al. (2006); 13, Sheu et al. (2006); 14, SingaporeCustoms (2011); 15, Thai (2007); 16, Thibault et al. (2006); 17, Timlen (2007); 18, Urciuoli et al. (2010); 19, Voort et al. (2002); 20, Voss et al. (2009); 21, Yang (2010); 22, Pallis and Vaggelas (2007); 23, Goulielmosa et al., 2014.

The costs of security investments in IT, EDI and technological solutions can well be a burden to companies that do not have enough resources. In the long run, however, benefits should outweigh the initial costs of security investment.

Besides, the classification of the impacts into reported and proposed can also be used. Specifically, a significant number of research papers, government publications and industry reports provide a wide range of expected benefits and negative impacts, which shipping organizations may experience after the implementation of different maritime security measures. Additionally, some of the maritime security regulations, especially voluntary programmes, propose benefits that shipping companies will enjoy if they become participants of these programmes (CBP, 2001, 2002; EU, 2007; Singapore Customs, 2011; WCO, 2007). However, the real picture might be completely different. Therefore, it is necessary to distinguish clearly between proposed and reported impacts. To date, not much reported data exist about the obtained impacts from the implementation of maritime security requirements on organizational performance 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. Among them are Bichou (2011), Thai (2007), Gutiérrez et al. (2007), Yang (2010), Urciuoli, et al. (2010), Voss, et al. (2009), Peleg-Gillai, et al. (2006), Voort, et al. (2002). Besides, it is worth noting that the majority of the reported impacts can be referred to as a short-term category. It is explained by a short period of time that passed since the new security regime came into force. That is why in this study, all reported impacts are considered as short-term, but the proposed impacts might be short-term, as well as long-term.

Based on the review of the literature on the impacts of the implementation of maritime security requirements on organizational performance of shipping companies, Table 2.8 was composed. It shows the classification of the impacts on organizational performance with respect to several levels: negative and positive, short-term and long-term, and proposed and reported, where the reported impacts are considered as short-term and proposed impacts might include both short-term and long-term impacts.

Table 2.8 Summary of the impacts of implementation of security requirements on organizational performance of shipping companies

Positive Impacts		Negative Impacts	
Reported	Proposed	Reported	Proposed
<ul style="list-style-type: none"> • increase in revenue (10) • enhanced branding (9,13,15) • reduce of cost (9) • reduce of insurance cost (9) • reduce of transit time (12,13) • improved efficiency (10) • improved security: (10,15) <ul style="list-style-type: none"> - reduced pilferage (9,12,19) - reduced stowaways (17) - reduced attacks (17) - reduction in tampering (12) - reduction in damages (9,12) - reduction in smuggling (9) • security awareness (13,15,16) • cooperation btw company, port, gov-t (16) • reduced number of inspection (13,16) • priority for inspection (16) • better governance: (12) <ul style="list-style-type: none"> - better use of IT (15) - better document processing (10,15,16) - improved cargo handling (10,12) - improved manpower utilization (10,12) - improved inventory management (10) - better data management (10,12) • better problem response (9,12) • quicker recovery from accidents (9) • customers' satisfaction (10,12) • higher customer service (13) 	<ul style="list-style-type: none"> • enhanced branding (7,14) • increased competitiveness (2,7) • reduce of cost (2,3) • reduce of insurance cost (3) • reduce of transit time (2,3,6,19) • improved efficiency (1,14) • increased visibility (3,6,14,19) • increased liability (2) • improved security: (2) <ul style="list-style-type: none"> - reduced pilferage (1,6,7,14) • cooperation btw company, ports, gov-t (3,11) • reduced number of inspection (5,6,7,8,14) • priority for inspection (5,8) • better governance: (1) <ul style="list-style-type: none"> - better use of IT (1,11) - improved product handling (6) - better data management (3,6) • better problem response(6) 	<ul style="list-style-type: none"> • financial loss (16,21) • lower competitiveness (21) • reputation injury (21) • additional cost: (15,16,18,21) <ul style="list-style-type: none"> - higher salary (18) • longer process time: (18,21) <ul style="list-style-type: none"> - delays in container clearance (15,21) - congestions (21) • less reliability (18) • less flexibility (18,21) • risk of disclosure of sensitive information (21) • need for extra staff (15) • staff shore leave (17, 23) • extra workload (15,21) • security taxes, tariffs (19,22) 	<ul style="list-style-type: none"> • lower competitiveness (16) • additional cost: (1,2,3,11) <ul style="list-style-type: none"> - increase insurance premiums (12) • longer process time: (1,3,11,12) <ul style="list-style-type: none"> - delays in container clearance (1,4,11,12,19) - congestions (2) • need to share the information with gov-t (1,20) • risk of disclosure of sensitive information (4) • need for staff training (1,19) • security taxes, tariffs (11,16) • decline of late bookings (3)

Notes: numbers in brackets indicate following publications: 1, APEC (2002); 2, Banomyong (2005); 3, Bichou (2008); 4, Bryant (2009); 5, CBP (2001); 6, Crutch (2006); 7, Eyefortransport (2002); 8, Fletcher (2007); 9, Gutiérrez et al. (2007); 10, ISO (2007); 11, OECD (2004); 12, Peleg-Gillai et al. (2006); 13, Sheu et al. (2006); 14, SingaporeCustoms (2011); 15, Thai (2007); 16, Thibault et al. (2006); 17, Timlen (2007); 18, Urciuoli et al. (2010); 19, Voort et al. (2002); 20, Voss et al. (2009); 21, Yang (2010); 22, Pallis and Vaggelas (2007); 23, Goulielmosa et al., 2014.

Table 2.8 shows that some of the impacts of implementation of maritime security requirements on organizational performance of shipping companies are met in both columns – reported and proposed. It is observed from the table that the proposed impacts are different from those reported. Specifically, some of the proposed impacts were not found among the reported. Besides, there is a number of negative impacts experienced by shipping companies, which were not proposed nor expected. The presented picture is not absolutely accurate, since the table was composed based on the limited available information. Additionally, inaccuracy in the table may be caused by the difference in the way of obtaining the data and subjectivity of perception of the information by industry professionals and researchers. For example, one can consider the need to cooperate with the government as a positive impact (Thibault, et al., 2006), whereas others see it in a negative way, since there is a risk of disclosure of sensitive information (APEC, 2002). This problem leads to the question about objective and subjective performance measurement, which is discussed later in Section 2.4.3.

The important conclusion from Table 2.8 is that the implementation of security requirements does not always lead to positive impacts, even though they were proposed. Moreover, it may also have unexpected negative impacts on the organizational performance of shipping companies. The significant difference in the obtained results may be explained by the fact that the same security requirements are implemented in different ways by various companies. That is to say that the approach to the management of security chosen by shipping companies may lead to very different consequences. This opinion is supported by Gutiérrez (2007, p. 231), who believed the following:

although all the companies followed the same security guidelines, they did not implement the program in the same way and they didn't obtain the same benefits or the same degree of security risks' reduction.

That is why the effective management of security in shipping companies is an essential condition for achieving benefits and avoiding negative impacts of the implementation of maritime security requirements (Thai, 2007).

Additionally, several authors believe that it is important for managers of shipping companies to know and understand the possible impacts of the

implementation of maritime security requirements (Gould, et al., 2010; Williams et al., 2008). For example, Williams, et al. (2008, p. 276) opined that “as security measures continue to affect organizations, researchers should help them to better understand how SCS is impacting business.” Good knowledge of the consequences of implementation of security management may help shipping companies to decide how to invest in security, what requirements to comply with and how to choose the most effective management strategy for a particular shipping company (Gould, et al., 2010).

2.4.2. Organizational Performance of Shipping Companies

This section provides a review of the literature on organizational performance of shipping companies. Firstly, the definition of organizational performance is provided. Secondly, the general concept of organizational performance and its categories and indicators is discussed. Finally, performance indicators used to measure impacts of maritime security initiatives in shipping companies are presented.

As can be seen in the literature reviewed, there is no single definition of organizational performance. Williams (2008) in his PhD Thesis listed the definitions of performance provided by different authors. Some of them, together with other definitions found in various studies, are summarized in Table 2.9.

Table 2.9 Definitions of organizational performance given by different authors

Definition	Author, Year
How well an organization achieves its market-oriented goals as well as its financial goals	Lakhal (2009)
The actual output or results of an organization as measured against its intended outputs: goals and objectives	Skrinjar et al. (2008)
The operations ability to satisfy the desires of the company's major stakeholders.	Smith and Reece (1999) in Zulkifli (2010)
The measure of what degree the organization has reached the market and financial goals they have set for themselves.	Yamin et al. (1999) in Williams (2008)
The process of evaluating progress in comparison to a predetermined goal.	Rose (1995) in Williams (2008)
Quantifying efficiency and effectiveness of actions.	Neely, Gregory, and Platts (1995) in Williams (2008)

Source: combined from different sources

As seen from the definitions provided in Table 2.9, some of the authors classified organizational performance according to organizational goals and objectives, for example financial and market. Similarly, if one of the objectives is to improve security, the organizational performance might be classified with consideration of the security performance. Thus, for the purpose of this study, the reviewed literature is organized into two groups, general literature on organizational performance and papers studying impacts of maritime security on organizational performance in shipping and supply chain companies.

The first group includes papers studying organizational performance in general and in the context of supply chain management, but not related to security. Generally, the classifications of organizational performance found in different sources are similar, however they might include different categories or indicators. The most commonly used category is *financial performance*, which is sometimes also called *firm performance* (Brewer and Speh, 2000; Choe et al., 1997; Cleveland et al., 1989; Evans 2007; Feng et al., 2008; González-Benito, 2007; Green et al., 2008; Raju and Lonial, 2001; and Tracey et al., 2005)). It usually contains the following performance indicators: profit, return on investment (ROI), return on assets (ROA), return on sale (ROS), profitability, cash flow, and profit-to-revenue ratio.

The second category, *market, marketing or commercial performance*, contains performance indicators such as market share, market growth, sales volume, sales growth, market development, new product/service development, competitive position, reputation and image, access to global market. These indicators were reported in studies of Choe et al. (1997), Cleveland et al. (1989), Evans (2007), Feng et al. (2008), González-Benito (2007), Green et al. (2008), Raju and Lonial (2001), and Tracey et al. (2005).

Several studies contain categories of organizational performance with similar performance indicators, such as quality, cost, productivity, flexibility, dependability, delivery speed, employee turnover, efficiency, response time, defect rate, delivery failure, variety of service, shipment accuracy, internal procedures, employee morale (Brewer and Speh, 2000; Choe, et al., 1997; Cleveland, et al., 1989; Feng, et al., 2008; Green, et al., 2008; Mann and Kehoe, 1994; Raju and

Lonial, 2001). The category containing the listed performance indicators is called differently: *operational performance* (Feng, et al., 2008; Mann and Kehoe, 1994), *manufacturing performance* (Choe, et al., 1997; Cleveland, et al., 1989), *internal business performance* (Brewer and Speh, 2000), *logistics performance* (Green, et al., 2008), and *quality outcomes* (Raju and Lonial, 2001).

The fourth commonly met category is *customer performance* with the following indicators: customer relationship, customer satisfaction, number of customer contact points, customer retention rate, and customer commitment (Brewer and Speh, 2000; Evans, 2007; Tracey, et al., 2005). There are a few other categories of organizational performance found in the related literature, such as *innovation and learning perspective* (Brewer and Speh, 2000), *preserved product value* (Tracey, et al., 2005), *human resource, supplier and partner performance* (Evans, 2007), and *strategic business performance* (Mann and Kehoe, 1994).

Bichou and Gray (2004) in their paper about a logistics and supply chain management approach to port performance measurement used the following indicators for performance evaluation: financial, economic impact, throughput, and productivity. In addition, several authors do not classify organizational performance into categories, however they list performance indicators (Gunasekaran et al., 2004; Han et al., 2007; Lakhal, 2009; Pinar and Girard, 2008; Zulkiffli, 2010; Skrinjar, et al., 2008). The most commonly mentioned indicators include profitability, market share (growth), sales (growth), return on investment (growth), return on assets, net profit, market development, overall competitive position, product/service quality, lead time, personnel turnover, relationships with suppliers, customer relations, number of new customers, etc. Table 2.10 summarizes the information found in the literature, and shows four most commonly met categories with indication of all possible names. It also displays studies from the second group of the reviewed literature, which will be discussed further.

As can be seen from Table 2.10, there are four most common categories of organizational performance found in the literature, namely *financial*, *market*, *internal business* and *customer performance*. This categorization was also used by Williams (2008) in his study on outcomes of supply chain security, where organizational performance was classified into *firm*, *market*, *customer* and *supply*

chain performance. This study is included in the second group of the reviewed literature, which combines papers on impacts of maritime security on organizational performance of shipping and supply chain companies.

However, the review of other studies from this group shows that for the purpose of measuring the impacts of security on organizational performance, not all four categories are applied. The literature in this group mostly contains performance indicators belonging to internal business performance and customer performance. Customer performance indicators, including customer service and customer relationships, were mentioned in the studies of Peleg-Gillai, et al. (2006) and Thai (2007). Internal business performance indicators, such as quality, costs, reliability, flexibility, visibility, efficiency, resilience, transit time, on-time delivery, safety, risk, and security, were reflected in papers of Urciuoli et al. (2010), Banomyong (2005), Thai (2007), Thibault, et al. (2006), and Peleg-Gillai, et al. (2006). Although security and safety indicators are listed in these studies, they are not detailed enough to measure improvements in these areas.

Nevertheless, there are a few studies where security and resilience indicators were grouped in separate categories. Gutiérrez et. al (2007) in their study on the benefits of joining the BASC (Business Anti-Smuggling Coalition) program classified them into three categories, namely *Direct security*, *Efficiency under normal conditions*, and *Efficiency under high alert/post disaster conditions*. The indicator of *Direct security* includes anti-smuggling, anti-theft, anti-loss and damage, anti-counterfeit, and others. The indicator of *Efficiency under high alert/post disaster conditions* contains quick recovery from direct disaster, quick recovery from general disaster, and others. Similar indicators, such as shorter problem resolution time, quicker response to a problem, and reduced time to identify a problem, were used by Crutch (2006) to describe collateral benefits of supply chain security on the category of *Resiliency*. Besides *Resiliency*, the author also distinguished categories of *Efficiency*, *Visibility*, and *Inventory Management and Customer Relations*. However, in both studies, the lists of indicators are not comprehensive enough in comparison with indicators of organizational performance, listed in Table 2.10.

Table 2.10 Categories of organizational performance found in the literature

Category of organizational performance	Performance indicators	Sources	
		General studies	Studies on supply chain and maritime security
Financial performance/ Firm performance	<ul style="list-style-type: none"> • profit, • ROI, • ROA, • return on sale, • profitability, • cash flow, • profit-to-revenue ratio; 	Cleveland et al. (1989); Choe et al. (1997); Brewer and Speh (2000); Raju and Lonial (2001); Bichou and Gray (2004); Tracey et al. (2005); Evans (2007); González-Benito (2007); Feng et al. (2008); Green et al. (2008).	Williams (2008)
Market performance/ Marketing performance/ Commercial performance	<ul style="list-style-type: none"> • market share, • market growth, • sales volume, • sales growth, • market development, • new product/service development, • competitive position, • reputation and image, • access to global market; 	Cleveland et al. (1989); Choe et al. (1997); Raju and Lonial (2001); Tracey et al. (2005); 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	<ul style="list-style-type: none"> • 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. 	Cleveland et al. (1989); Mann and Kehoe (1994); Choe et al. (1997); Brewer and Speh (2000); Raju and Lonial (2001); Bichou and Gray (2004); Feng et al. (2008); Green et al. (2008).	Banomyong (2005); Peleg-Gillai, et al. (2006); Thibault, et al. (2006); Thai (2007); Williams (2008); Urciuoli et al. (2010).
Customer performance	<ul style="list-style-type: none"> • customer relationship, • customer satisfaction, • number of customer contact points, • customer retention rate, • customer commitment; • knowledge of customers' needs. 	Brewer and Speh (2000); Tracey et al. (2005); Evans (2007).	Peleg-Gillai, et al. (2006); Thai (2007); Williams (2008).

Source: author, adapted from various sources

2.4.3. Measurement of Impacts of Maritime Security Management on Organizational Performance of Shipping Companies

Many publications studying the objective and subjective approaches to the measurement of organizational performance have been found. The reviewed publications did not solely focus on the performance of organizations in the supply chain, but also examined performance measures in general. Generally, measures of organizational performance are divided into subjective and objective, whereas, some authors also indicated that subjective measures can be fully subjective and quasi-objective (Richard et al., 2009). Objective measures “refer to performance indicators impartially quantified” (González-Benito and González-Benito, 2005, p. 802). “Subjective measures ask supposedly well-informed respondents (key informants) about organizational performance” (Richard, et al., 2009, p. 735). Quasi-objective measures are used to ask opinions on some objective information regarding organizational performance. Organizational performance is measured subjectively by using “a scale with anchors such as “very poor” to “very good”, or “much lower” to “much higher” compared to competitors”, whereas objective measure is “an actual percentage figure for sales growth or profitability” (Dawes, 1999, p. 1).

It is interesting to find out what measures are commonly used for the evaluation of organizational performance of every category: financial performance, market performance, internal business performance, and customer performance. A comprehensive work has been done by Richard, et al. (2009) in reviewing of publications on performance measures, published for the period from 2005 till 2007 in the following five journals: Academy of Management Journal, Administrative Science Quarterly, Journal of International Business Studies, Journal of Management, and Strategic Management Journal. It was observed that a majority of the measures related to internal business performance and customer performance were subjective, whereas, financial and market performance were measured subjectively, as well as objectively. This observation was also supported by literature reviews done by Dawes (1999) and González-Benito and González-

Benito (2005). One of the possible reasons is that objective measures cannot always be found for every area of organizational performance (Richard, et al., 2009).

However, it is suggested that the use of subjective measures is not considered as the second-best option by researchers (Richard, et al., 2009). Many studies have been conducted on the correlation between subjective and objective performance measures, and the findings showed that subjective measures may be used in the absence of objective measures (Dawes, 1999; Dess and Robinson, 1984; Richard, et al., 2009). Moreover, Richard, et al. (2009) indicated that the increased interest of researchers in using subjective measures was observed in recent years.

There are several reasons for using subjective measures. Firstly, objective measures are often difficult to obtain and are not always reliable, because of the unwillingness of managers to disclose commercially sensitive or confidential information or simply because of the lack of time on the part of the managers (Dawes, 1999; González-Benito and González-Benito, 2005; Neely et al., 2006). Secondly, some objective measures of financial performance in the short-term approach may not accurately indicate organizational performance (Dawes, 1999; Neely, et al., 2006). Lastly, subjective measures are more applicable for cross-industry analysis and cross-sectional analysis through sectors and markets, as their use facilitates measurement of complex dimensions of performance (González-Benito and González-Benito, 2005).

However, subjective measures are often considered as biased by managers and researchers. Their bias may lead to unreliability of the obtained results. For example, respondents may tend to view themselves positively or provide positive responses to enhance the company's image, what leads to "false positive" findings (Boyne, 2006; Dawes, 1999; González-Benito and González-Benito, 2005; Richard, et al., 2009). It is believed that proper research design helps to avoid the bias. For example, selecting well-informed respondents, defining used items clearly, and collecting information as close to the event as possible, may help to reduce an error (Richard, et al., 2009). Additionally, adopting a combination of subjective and objective performance measures is another approach to increase objectiveness of results (Boyne, 2006).

It is observed that in shipping and supply chain related literature, subjective measurements of organizational performance are much more applicable than objective. The most often used approaches are survey-based self-reports, questionnaires, in-depth interviews with industry professionals, and workshops. When designing a questionnaire, the Likert scale is frequently applied. Most commonly, changes in organizational performance are measured by comparing it before and after the implementation of security measures, or over a specified period of time. Some authors checked whether or not these changes were observed in the company (Thai, 2007; Voort, et al., 2002), others measured the significance of these changes (Bichou and Gray, 2004; Gunasekaran, et al., 2004; Voss, et al., 2009).

Peleg-Gillai, et al. (2006), in their study about supply chain security, used percentage evaluation of changes in organizational performance. A comparison of organizational performance with competitors' or with industry average performance was also applied in several studies (Green, et al., 2008; Zulkiffli, 2010; Williams, 2008). Gunasekaran, et al. (2004) used a comparison between expected and obtained benefits in a proposed framework for supply chain performance measurement. Additionally, this study led to thoughts about comparing organizational performance with some industry norms, such as the delivery time or loading time. According to Gunasekaran, et al. (2004, p. 334), "to meet the objectives, the output of processes enabled by the supply chain must be measured and compared with a set of standards." Gutiérrez, et al. (2007) in their study about the implementation of BASC initiatives compared expected and obtained benefits. Yang (2010) measured the impacts of container security initiatives on organizational performance of the shipping industry by evaluating the frequency and severity of observed impacts. Among all mentioned approaches to performance measurement, the two approaches most commonly found in general literature are comparison to competitors and comparison over time to changing conditions (absolute performance) (Bhatnagar and Sohal, 2005; Dawes, 1999; González-Benito and González-Benito, 2005).

However, some studies based on the objective measurement of organizational performance in shipping companies were also found. Bichou (2011) used

Malmquist Data Envelopment Analysis (DEA) for assessing the impact of procedural security on container port efficiency. He examined the changes in terminal efficiency, scale efficiency, pure technical efficiency, and technological changes. DEA was developed by Charnes, Cooper, and Rhodes (1978), and “in this method, multiple inputs and outputs could be used to measure an entity’s performance” (Mohammadi and Ranaei, 2011, p. 69). However, as mentioned earlier, sometimes it may be difficult to obtain the information necessary for objective performance measurement. It can be given by companies’ managers or it can be taken from secondary sources, such as annual reports, usually posted on the company’s website. That is why, the use of the objective measurement approach exclusively is not recommended for the organizational performance measurement (Boyne, 2006).

Taking into account the possible problems related to objective measurement, it might be suggested that the combination of subjective and objective performance measures is used (Boyne, 2006). If objective measures are not available, quasi-objective measures can be a good alternative. Additionally, to weaken the bias of the results, the combination of subjective approaches can be used. Thus, respondents can be asked to compare organizational performance before and after the implementation of security initiatives, as well as to compare it to their main competitors or industry average. Moreover, the percentage evaluation may also be applicable for clarification of the results. The combination of approaches to performance measurement was found in several publications reviewed by González-Benito and González-Benito (2005) and Richard, et al. (2009), however no similar papers were found among maritime security related literature. Thus, to achieve more reliable results, the combination of objective and subjective approaches for the measurement of organizational performance of shipping companies is applicable in this research.

2.5. Summary of Literature Review

The current chapter of this report provides a review of the literature on three interconnected topics according to the research questions. They are maritime security regulations and requirements for shipping companies, effective management of maritime security in these companies, and impacts of maritime security management on their organizational performance. Even though the topic of maritime security is comparatively young, the contributions by researchers in this field in the last several years have been significant. Nevertheless, there is still a big area for further research and development.

For the first research question, the regulatory documents relevant to maritime security were reviewed. After that, a review of other government documents, industry reports and scientific publications was conducted. A long list of publications discussing various maritime security regulations and requirements was found. However, it was observed that no studies have been conducted on summarizing all the security regulations and requirements for shipping companies. Moreover, not many researchers studied the practical implementation of these requirements, even though this information may become a significant contribution to studies on effective maritime security management in shipping companies. To fill the identified gaps, for the purpose of the first research question, the following has been done:

- Maritime security regulations were carefully examined (Table 2.1) and a comprehensive list of compulsory and voluntary security requirements for shipping companies was developed (Tables 2.2 and 2.3);
- The current issues with existing maritime security requirements, including overlapping and inconsistency, were examined;
- The review of the literature on the implementation of the requirements showed that there is a lack of studies on this topic and further research is necessary.

Literature for the second research question on management of security in shipping companies was reviewed next. Not many publications, focusing on security management in shipping companies, were found. Thus, the list of reviewed literature was widened by including studies on supply chain security. The literature

showed that shipping companies still have difficulties with managing security, and the proposed models and frameworks do not address all these difficulties. The results of the literature review on the second research questions are summarized as follows:

- The management approaches applicable to maritime security management were carefully examined (Table 2.4);
- Review of the models and frameworks for maritime security management proposed by other researchers was conducted to identify their strengths and weaknesses, which can be further applied for the development of the EMSMM;
- Current issues of maritime security management in shipping companies were discussed;
- A list of essential criteria for the EMSMM was composed based on the reviewed management approaches, models and frameworks, and examined problems (Table 2.5).

The last section of this chapter provides literature review on the impacts of security management on organizational performance of shipping companies. It can be seen from the reviewed literature that there is no clear understanding on how management of maritime security can impact organizational performance of shipping companies, since limited reported information is available. Besides, there is no specific scale including categories and indicators of organizational performance, which can be applicable for measuring the impacts of security management in shipping companies. To address the identified gaps, for the literature review on the third research question, the following has been done:

- A list of impacts of security management on organizational performance of shipping companies, available in the literature, was composed with the consideration of the following criteria: positive and negative, short-term and long-term, and reported and proposed impacts (Table 2.8).
- A list of the most commonly met categories of organizational performance and their indicators was composed based on the general literature on organizational performance (Table 2.10).

- The categories and indicators used for security management in maritime and supply chain related literature were studied to later develop the scale for shipping companies.
- The measurement of the impacts on organizational performance of shipping companies was discussed.

It can be concluded that this chapter provides answers to sub-questions 1.1, 1.2, 2.1, 2.2, 2.3, 3.1 of this study. Besides, it prepares a good background for further research on other research questions of the study. However, besides the gaps, which have been already been discussed in the literature review, there are some other identified gaps, which will be addressed in the next two chapters of this research. Table 2.11 summarizes the gaps and shows the ways to address them.

Table 2.11 Gaps of the reviewed literature and solutions

Literature Gaps	Solutions
No studies have been conducted to review and summarize all security regulations and requirements for shipping companies.	Table 2.1 provides a list of maritime security regulations for shipping companies. Tables 2.2, 2.3 provide comprehensive lists of maritime security requirements imposed on shipping companies.
Not many studies have been conducted on the implementation and effectiveness of the security requirements in shipping companies;	The gap needs to be addressed in this research.
Not many studies focused on management of security in shipping companies.	Section 2.3 provides a detailed review of the literature on maritime security management in shipping companies.
Not all of the existing problems are considered in the proposed security management models and systems.	Based on the existing problems the list of essential criteria for the EMSMM was composed and presented in Section 2.3.4. The EMSMM, developed and validated in this research, should satisfy the criteria. It is expected to help solving the problems.
The balance between security, efficiency and resilience is seldom taken into consideration in the proposed security management models and systems.	The EMSMM, proposed and validated in this study, is expected to help in achieving a balance between security, efficiency and resilience.
No studies have been conducted to summarize impacts of security management on organizational performance of shipping companies.	Table 2.8 summarizes impacts according to several criteria, namely, positive and negative impacts, reported and proposed impacts, and short-term and long-term impacts.
Majority of studies on organizational performance do not use detailed enough performance indicators for security and resilience measurement. Whereas, in some other studies, where security and resilience indicators are detailed and presented in separate categories, the list of other organizational performance is not comprehensive and does not include a number of indicators from other categories.	The gap needs to be addressed in this research.
Limited information has been found on the approach to measure impacts of security management on organizational performance.	Section 2.4.3 provides a discussion on measurement of impacts of maritime security management on organizational performance of shipping companies.
The studies, which propose maritime security management models and systems for shipping companies, have not examined relationships between security management and organizational performance.	The gap needs to be addressed in this research.

CHAPTER 3. METHODOLOGY

3.1. Introduction

The purpose of this chapter is to present and describe the methodology applicable in this study. The chapter begins with a list of research questions and sub-questions and a brief discussion about them. Based on the discussed research questions, the detailed objectives are then stated, followed by the explanation on the research approach used to answer the research questions. The next section of the chapter presents the detailed research process and gives an overview about the methods used to answer each research question. The model development is discussed next. The chapter continues with a discussion of the various methods of data collection, population and sampling frame, and data editing, coding, categorising and entering process. The methods of data analysis are then described. The chapter ends with a discussion on the possible errors and ways to reduce them.

3.2. Research Questions

As discussed earlier, this study aims to address three main research questions (RQ) with several sub questions (SRQ) each. The first research question is important to provide a regulatory foundation for the developed model. Answers to this question explain the need and background for the development of the EMSMM. The first research question and its sub-questions are formulated as follows:

RQ1. What are the existing maritime security regulations and requirements for shipping companies?

SRQ1.1 What regulations currently exist in the field of maritime security?

SRQ1.2 What maritime security requirements are imposed on shipping companies?

SRQ1.3 What maritime security requirements are implemented in shipping companies?

The second research question and its sub-questions are essential to achieve the second aim of this study. The answers to the following questions provide a significant contribution to the development of the EMSMM and its factors:

RQ2 How can maritime security be managed effectively in shipping companies?

SRQ2.1 What management approaches and models are applicable to manage maritime security effectively?

SRQ2.2 What problems of security management do shipping companies currently face?

SRQ2.3 What are the essential criteria for the EMSMM?

SRQ2.4 What are the factors of the EMSMM?

Finally, to understand why the proposed EMSMM is important and meaningful, the third research question and its sub-questions are formulated as follows:

RQ3 What are the impacts of maritime security management on organizational performance of shipping companies?

SRQ3.1 What are the reported and proposed impacts of the implementation of maritime security initiatives on organizational performance of shipping companies?

SRQ3.2 How do the EMSMM and its factors impact organizational performance of shipping companies?

3.3. Research Approach

Because of the nature of the topic, a combination of exploratory, descriptive and causal research approaches is applied in this study. Exploratory research approach is conducted when no or few studies have been done in the studied area (Dawson, 2002). The exploratory research is often used to test proposed concepts or models before they are put in the market. As can be seen from Section 2.3, there are very few studies conducted on maritime security management in shipping companies. Table 2.5 shows that none of the existing maritime security management models or systems for shipping companies satisfies the essential

criteria. Since the proposed EMSMM is developed and validated for the purpose of this study and presents a new concept, the exploratory research approach is applied.

Descriptive research approach is conducted to describe a population or situation with respect to important variables (Jackson, 2009). In this study, the descriptive research approach is applied to collect and analyze the information about implementation and effectiveness of security requirements in shipping companies, about how the companies manage maritime security, and about changes in their organizational performance. The methods of data collection, such as survey, interviews, case studies, are often applicable in descriptive research.

Finally, the causal approach is conducted to explore the effect of one variable on another (Markus and Robey, 1988; Venkatraman and Ramanujam, 1986). In this study, the causal approach is used to study the relationship between the proposed EMSMM and organizational performance of shipping companies, where the factors of the model are used as independent variables and categories of organizational performance are considered as dependent variables.

3.4. Research Process

This research has three main research aims. The first aim is to study the maritime security regulations and requirements imposed on shipping companies. The second aim is to develop and validate the EMSMM for shipping companies. The third aim is to understand the impacts of maritime security management on organizational performance of shipping companies. Each aim helps to answer different research questions and examines separate problems. However, all of them are closely related to one another and similar methods are used to achieve different aims. Therefore, the research process is divided into several stages according to the research methods.

At the literature review stage, the review of documents regulating security in shipping companies was first conducted to contribute to the first aim of the research. Since shipping companies are essential elements of the supply chain, the various supply chain security programs were also included. After a detailed study of the compulsory and voluntary regulatory documents, a review of security

requirements was conducted. Simultaneously, a number of government and industry reports, as well as scientific publications, were reviewed to increase the understanding on the studied area. Based on the reviewed literature, a comprehensive list of compulsory and voluntary security requirements for shipping companies was composed. Then to achieve the second aim of this research, the related literature was reviewed to study the existing approaches to maritime security management, as well as proposed models and systems of security management in shipping companies. Moreover, the common problems in this area were identified, and a list of essential criteria for the EMSMM was composed. Lastly, as a contribution to the third aim, a comprehensive literature review was conducted to classify organizational performance and identify performance indicators in shipping companies. Moreover, based on the related literature, such as research papers, government and industry reports, a list of proposed and reported impacts of the implementation of security initiatives on various organizational performance of shipping companies was composed.

Further at the stage of model building, the list of essential criteria composed during literature review was used to develop the EMSMM and its factors. The factors were derived with consideration of the main principles of approaches used for security management, and each factor satisfies one or more essential criteria. Besides, based on the comprehensive review of literature on organizational performance, the reviewed indicators were classified into three categories for the purpose of testing relationships between the EMSMM and organizational performance of shipping companies.

Following the literature review and model building, the next stage was to conduct exploratory interviews to examine the studied problems in more details before conducting the survey. The interviewees were asked to provide their opinion on different questions, namely the implementation and effectiveness of security requirements in their companies, the importance of the factors of the proposed EMSMM, and observed changes in the organizational performance of their companies. The exploratory interviews helped to answer the research question 1.3 and resulted in some changes in the proposed model.

The amended model was further used to conduct a main survey. At the stage of the main survey, the data were collected to contribute to the second and the third research aims. Validation of the model was carried out by analysing the data collected through the survey. Besides, the data were collected to measure the impacts of the proposed model and its factors on the organizational performance of shipping companies participating in the survey. The stage of the main survey resulted in the validated EMSMM. The relationship between the model's factors and categories of organizational performance were tested and explained.

Finally, to confirm the results of the main survey and prioritise the model's factors, the confirmatory survey was conducted based on the analytic hierarchy process (AHP) technique. As discussed in Chapter 2, a combination of the listed methods helps to reduce the subjectivity of the collected data, but at the same time widens the range of available information. Figure 3.1 shows the research process and methods used to answer every research question of the study. Similarly, Table 3.1 shows the phases of the research process and results of each stage according to three research aims.

Figure 3.1 Research process

Table 3.1 Summary of research stages and results according to aims

Research Stages	Results according to research aims		
	<i>Aim 1</i> <i>Study of maritime security regulations and requirements for shipping companies</i>	<i>Aim 2</i> <i>Development and validation of the EMSMM for shipping companies</i>	<i>Aim 3</i> <i>Understanding of impacts of maritime security management on organizational performance of shipping companies</i>
<i>Literature Review</i>	<ul style="list-style-type: none"> List of regulatory documents containing requirements for shipping companies Comprehensive list of compulsory and voluntary maritime security requirements for shipping companies 	<ul style="list-style-type: none"> Review of the existing approaches and proposed systems, models and frameworks of security management Identification of problems of security management in shipping companies List of essential criteria of the EMSMM 	<ul style="list-style-type: none"> List of reported and proposed impacts of implementation of security initiatives on organizational performance of shipping companies Categories and indicators of organizational performance of shipping companies
<i>Model Building</i>	-	<ul style="list-style-type: none"> Development of model's factors and their attributes 	<ul style="list-style-type: none"> Categorization of the organizational performance of shipping companies Indicating the tested relationship between the model's factors and categories of organizational performance
<i>Exploratory Interviews</i>	<ul style="list-style-type: none"> General view of interviewees on maritime security regulations for shipping companies Implementation and effectiveness of maritime security requirements in the interviewed companies 	<ul style="list-style-type: none"> Implementation and effectiveness of the EMSMM's factors in the interviewed companies Amended EMSMM according to interviewees' comments 	<ul style="list-style-type: none"> Negative and positive impacts, observed in the interviewed shipping companies
<i>Main Survey</i>	-	<ul style="list-style-type: none"> Validated and confirmed EMSMM 	<ul style="list-style-type: none"> Impacts of the EMSMM and its factors on organizational performance
<i>Confirmatory Survey</i>	-	<ul style="list-style-type: none"> Prioritisation of the EMSMM's factors based on their importance 	-

3.5. Model Building and Hypotheses Development

The proposed effective maritime security management model (EMSMM) contains nine factors, logically deduced from the existing literature on maritime security management. As discussed earlier, the EMSMM should satisfy several important criteria: to manage the balance between security performance, business resilience and other organizational performance; to help in the implementation of the compulsory and voluntary security requirements; to be based on a holistic approach to security management; as well as to be flexible and easy for implementation. Thus, to satisfy the listed criteria, some of the factors were partly derived from the existing models and frameworks for security management, while others were developed based on the principles of the management approaches commonly used for security management. Besides, some of publications were discussing the existing and potential problems or mentioned the necessity to focus more on specific areas. These publications were also reviewed and cited as literature sources when developing the model's factors. Moreover, the existing compulsory and voluntary requirements for shipping companies were taken into consideration at every step of the literature review and development of factors of the model and their attributes. The process of deriving the model's factors is shown in Figure 3.2.

Figure 3.2 Process of deriving the EMSMM's factors

The EMSMM contains the following nine factors, namely *Security Culture*; *Management and Employee Commitment*; *Security Assessment*; *Security Policy, System and Procedures*; *Documentation and Communication*; *Process Control*; *Continuous Security Improvement*; *Security Incidents Handling and Continuity of Operations*; and *Business Partners Security*. Figure 3.3 shows the EMSMM and its factors. The model's factors and the components, composing the factors, are discussed below.

Figure 3.3 Factors of the EMSMM

The first factor of the proposed model is *Security Culture* (Gould, et al., 2010; Voss, et al., 2009; Williams, et al., 2009). Williams, et al. (2009, p. 246) believed that the security culture in supply chain organizations

creates SCS as a priority among employees through embracing and projecting norms and values that support security-related activities and allows employees to be vigilant in undertaking SCS-related efforts.

This factor includes several components, such as Total organizational focus on security (ISO, 2000, 2005; Lee and Whang, 2005; Thai, 2009; Williams, et al., 2009), Security awareness among employees (Bichou et al., 2007; Gould et al., 2010; Thai and Grewal, 2007), Making security a part of organizational every day activity (Rice and Caniato, 2003a; Williams, et al., 2009), and Security related knowledge (Gutiérrez, 2007; Williams, et al., 2009). These components were mostly derived from principles of QM (or TQM), such as total organizational focus on security, security awareness, and process control and management for security purposes; as well as from principles of BCM, such as security related knowledge and culture, knowledge management, and periodical security training. In combination, these principles help to achieve a holistic approach to security management by integrating security into all activities in the organization, what satisfies the sixth essential criteria for the EMSMM.

Management and Employee Commitment is the second factor of the EMSMM (Bichou, et al., 2007; Thai, 2009). This factor helps to involve all of the organization's employees in security management according to their responsibilities and positions. It helps to fill the existing security gaps in the organization and make security management more structural. It includes several components: Clearly defined security accountability and responsibility (Thai, 2009; Gutiérrez, 2007), Security related decision making (Bichou, et al., 2007), Security improvement team (Bichou, et al., 2007), Management commitment and security training (Bichou, et al., 2007; Thai, 2009), Employee empowerment and commitment (Bichou, et al., 2007; Thai, 2009), and Investing in security. Principles of QM include the development of the improvement team, involvement of employees in company management; clearly identified decision makers, and training for management. These principles, together with principles of BCM, such as the hierarchy in the organization (for security management) and periodical training of employees, were used to derive components of the second factor. Similarly to the first factor, the

second one helps to satisfy the sixth essential criterion by involving all employees into security management.

The third factor is *Security Assessment*. This factor is essential to establish the security level in a shipping company and the measures required to achieve and maintain this level (Bernard, 2009; Rice and Tenney, 2007). It also helps to understand the environment in which security threats are derived. It includes several components: Risk identification and assessment (Thai, 2009; UNCTAD, 2006); Assessment of the level of compliance with security requirements (Bernard, 2009; Rice and Tenney, 2007); and Measures adjustment and investing in security according to risk (Rice and Caniato, 2003a; Thai, 2009; Sarathy, 2006; Sheffi, 2008). These components were derived, based on the principles of existing management approaches, identified gaps in the security related literature and essential criteria of the EMSMM. The first component, Risk identification and assessment, comes from the principles of RM, such as risk identification and risk assessment. Two of the essential criteria require the proposed model to be developed specifically for shipping companies and to be flexible for application. To satisfy these criteria, every single organization shall conduct risk identification and assessment with consideration of risks and features of this organization. Second component, Assessment of the level of compliance with security requirements, is necessary for the implementation of compulsory and voluntary security requirements, which is another essential criterion of the model. This component was derived from a principle of RM, assessment of level of compliance. Moreover, one of the identified problems of maritime security management is that proposed models often do not include the evaluation of the impacts of security management on the organizational performance, as well as that they do not advice the follow-up actions (the fifth essential criterion). To satisfy the mentioned criterion, the third component of the factor, Measures adjustment and investing in security according to risk, were derived based on principles of QM, such as the establishment of performance standards, measures adjustment; and the principles of a layered approach, including investing in security according to the risk. Therefore, the model does not force companies to use any single strategy for risk assessment, however it suggests them to include this procedure into a daily routine.

Another factor of the model is *Security Policy, System and Procedures*. A well-developed and timely reviewed security management system, including policies and procedures for all security-related processes and activities in the organization, helps to achieve transparency in security management and other security related operations for the organization's employees and management. The policy should be detailed and developed with consideration of all features of a shipping company. Additionally, it should stimulate and manage the implementation of various security measures, including compulsory and voluntary security requirements. Based on that, the following components of the fourth factor were derived: Development of well-structured security policy and procedures and their periodical reviewing (Thai, 2009; Williams, et al., 2008) and Business continuity plans and emergency plans and their periodical reviewing (Gould, et al., 2010). The principles of several management approaches form the basis of the components. For example, development of the security policy, strategies and plans is a Do-step in a PDCA cycle, introduced by Thai (2009) as an application of QM for security management (please refer to Figure 2.2). Besides, development of the internal policies to prepare for security incidents, as a principle of TSM, as well as development of contingency and emergency plans, and documentation management, as BCM principles, was also used for deriving the components of the fourth factor.

Documentation and Communication is the fifth factor of the model (Autry and Bobbitt, 2008; Closs, et al., 2008; Gould, et al., 2010; Thai, 2009). Many of the existing regulations require shipping companies to collaborate with other participants of the supply chain, as well as with the government. The documentation exchange and maintenance is an important part of the communication. To secure this area of organizational activities, necessary security measures should be taken. This factor includes several components, such as Communication with business partners and governments for security purposes (Thai, 2009; Closs, et al., 2008), Backup of communication systems (Russel and Saldanha (2003) in Williams, et al., 2008), Information security and backups (Rice and Caniato, 2003a; Closs, et al., 2008; Thai and Grewal, 2007), Data management (Gutiérrez, 2007), and IT and financial security. The components were derived from the principles of BCM and layered approach, such as backups of documentation system, development of the

information system with alternative communication system backup, collaboration with partners and government for security purposes, etc. Implementation of security measures, such as communication backup systems and backup of documentation, is a part of preparation process for handling security incidents. Thereby these measures help the organization to increase its level of resilience, which is the fourth essential criterion of the model. Moreover, the communication processes involve many different parties, therefore to manage security of communication, the holistic approach to security management shall be applied.

The next factor of the model is *Process Control*. This factor has been discussed in earlier studies such as those of Thai (2009) and Closs et al. (2008), and its components were mostly derived from the principles of TQM, such as process control for security purposes, systematic improvement of working processes, and creating visibility. This is elaborated in Thai (2009, p. 148) who argued that

similarly [to quality management], 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 with.

Additionally, the process control for monitoring shipment may be expanded to the control of all processes and activities in the organization for security purposes. By doing this, a holistic approach to security management may be achieved. Besides, the process control may be useful in achieving some collateral benefits, which in turn helps to increase efficiency. Finally, all processes in the shipping company should be carefully identified and described, as well as periodically reviewed and improved. Some of the processes are unique and exist only in shipping companies. The identification and control of these processes make the model more flexible and suitable for different types of shipping companies. Based on the discussed principles the following components of the sixth factor were derived: Security prevention from the source, Process control and management for security purposes, Systematic reviewing and improvement of working processes, and Creating visibility (Gould, et al., 2010; Gutiérrez, 2007; ISO, 2000, 2005; Lee and Whang, 2005; Thai, 2009).

The seventh factor, *Continuous Security Improvement*, has been discussed by several researchers focused on security management, such as Bichou, et al. (2007) and Thai (2009). To achieve the required security level, it is necessary to ensure a constant revision of all security related activities and processes in the organization, as well as the application of all required follow-up measures. Therefore, a continuous security improvement ensures a constant link between security management and its impacts on the organizational performance, which satisfies the fifth essential criterion of the EMSMM. Whereas, the necessity to evaluate a compliance with security requirements is the second essential criterion. Components of the factor were mostly derived from the principles of TQM and RM. The first component, Periodical assessment of security management system and its elements, is based on principles of RM, such as risk identification and risk assessment, and is necessary to identify current level of security in the organization (ISO, 2000, 2005; Lee and Whang, 2005; Thai, 2009). The second component, Correction actions and error cause removal, is important for follow-up improvement actions and was derived from the principles of TQM, such as process control and management for security purposes, continuous security improvement, preventing and mitigating verification, corrective actions, and error cause removal (Bichou, et al., 2007; Sarathy, 2006).

The eighth factor, *Security Incidents Handling and Continuity of Operations*, is necessary to mitigate disruptions in the organizational processes (Gould, et al., 2010; Macdonald and Corsi, 2013; Thai, 2009; Williams, et al., 2009). It aims to increase the resilient ability of the organization's operations. Additionally, since the recovery actions should involve the organization itself, as well as its partners and government representatives, a holistic approach to security management is an important component of the factor. The components of the eighth factor are based on the following principles of BCM and layered approach: emergency plans for response to disruption, contingency planning, disaster recovery, development of backups, etc. The components include Business continuity and emergency plans and their periodical reviewing, Recovery plans (Thai, 2009; Sarathy, 2006), and Periodical security and disaster management training (Rice and Caniato, 2003a).

The last factor of the model, *Business Partners Security*, helps to extend the company's security to its suppliers and customers (Acciaro and Serra, 2013; Autry and Bobbitt, 2008; Closs, et al., 2008; Gould, et al., 2010; Gujar et al., 2013; Macdonald and Corsi, 2013; Thai, 2009). Since shipping company is an important component of the supply chain, security should be controlled not only within the organizations, but also outside. When every participant of the supply chain extends its security to its business partners, the supply chain would be secure. As discussed earlier, one of the current problems of security management is an existence of gaps in security regulations (Gould, et al., 2010; Thai and Grewal, 2007). Not all of the areas of shipping and supply chain are covered by existing regulatory regime. These gaps should be voluntarily secured by organizations of a supply chain. Collaboration between companies of the supply chain plays an important role. Partners should carefully discuss the possible threats and assess the risks, identify the security gaps. Based on that, they should distribute responsibilities to cover all identified security gaps, and discuss liability for possible security incidents (Gujar et al., 2012). The discussed responsibilities should be expressed in written and detailed policies, as well as emergency plans, business continuity plans and recovery plans should be jointly developed and exercised. This factor is based on principles of TQM, BCM, layered approach and RM. The involvement of various participants of supply chain helps to achieve a holistic approach to security management. The factor includes several components: Security assessment of business partners (Sarathy, 2006; Williams, et al., 2008); Clear distribution of responsibilities (to secure identified gaps) and liabilities between partners (Gujar et al., 2012); and Joint security trainings and exercises with business partners.

The nine listed factors of the proposed model, as well as their components, were partly derived from the existing compulsory and voluntary maritime security requirements for shipping companies. The components do not repeat the requirements, but they facilitate their implementation. Therefore, the factors and components of the proposed model help with implementation of the appropriate security requirements in shipping companies, which satisfies the second essential criterion of the model. Additionally, to satisfy the requirement that the EMSMM should be flexible and easy for implementation. The factors are listed in Table 3.2.

The table shows based on what management approaches each factor was derived and what essential criteria are satisfied by including this factor.

Table 3.2 Management approaches and essential criteria used to develop the nine factors of the EMSMM

Factors	Management Approaches	Essential Criteria
Security Culture	QM, BCM	6
Management and Employee Commitment	QM, BCM	6
Security Assessment	RM, QM, Layered approach	2, 3, 5, 7
Security Policy, System and Procedures	QM, BCM, TSM	2, 3
Documentation and Communication	BCM, Layered approach	4, 6
Process Control	TQM	3, 6, 7
Continuous Security Improvement	TQM, RM	2, 5
Security Incidents Handling and Continuity of Operations	BCM, Layered approach	4, 6
Business Partners Security	QM, RM, BCM	6
<i>All factors together</i>		1, 2, 7

At the next stage of the model development process the discussed components were elaborated by deriving associated attributes. These attributes were developed as guidance for the model's implementation, as required by the first essential criterion. Table 3.3 demonstrates the components of the model's factors, the literature sources used to develop these components as well as attributes associated with each component.

Table 3.3 Literature sources, components of the factors and associated attributes

The EMSMM's Factors	Components	Literature Sources	Associated Attributes
1. Security Culture	Total organizational focus on security	ISO (2000, 2005), Thai (2009), Williams, et al. (2009) Lee and Whang (2005),	Senior management promotes the security culture to inspire it throughout the organization.
			Implement a total approach for security management, similarly to quality or safety management.
	Security awareness among employees	Bichou, et al. (2007), Gould et al. (2010), Thai and Grewal (2007)	Conduct periodical trainings and seminars on security purposes to achieve security awareness.
			Allocate the necessary budget for propaganda of security in the organization and assign responsible personnel.
			Provide a clear explanation of the objectives of security measures and background information to promote the awareness in the organization.
	Making security a part of organizational every day activity	Rice and Caniato (2003a), Williams, et al. (2009)	Responsible personnel, as well as all organization's employees have to assure that all processes and activities in the organization comply with the established organizational standards.
2. Management and Employee Commitment	Security related knowledge	Gutiérrez (2007), Williams, et al. (2009)	Periodically distribute the security related information among employees through email, brochures, posters or video announcements.
	Clearly defined security accountability and responsibility	Gutiérrez (2007), Thai (2009)	Establish written and detailed procedures and responsibilities for all organization's employees.
			Timely inform every employee regarding his/her own responsibilities and corresponding changes, as well as regarding responsibilities of other employees (if appropriate).
	Security related decision making	Bichou, et al. (2007)	Clearly identify and document the process of security related decision making.
			Clearly identify the type of decisions, which can be made on different levels of the organization.
			Describe and document the procedure for communication between different levels in the organization (from decision maker to performer and back).
	Security improvement team	Bichou, et al. (2007)	Compose the security improvement team from managers of different departments, employees' representatives and, if possible, government consultants.

			Team works on development and implementation of security standards, makes security related decisions on the highest level of the organization, and discusses all other security related questions.
			Include employees' representatives to the security improvement team.
	Management commitment and security training	Bichou, et al. (2007), Thai (2009)	To promote security culture in the organization managers need to have a deep understanding of security measures and regulations and their background.
			Organize security related trainings outside the organization for managers of the organization.
	Employee empowerment and commitment	Bichou, et al. (2007), Thai (2009)	Develop easy procedures for employees on different levels of the organization to provide their feedback regarding security related issues.
			Establish a Reward & Recognition program to motivate employees providing a feedback on security issues.
			Involve employees from different levels of the organization into process of development of the security policy and procedures.
	Investing in security	NA	Senior management considers security investments as a service quality improvement facilitator.
			Senior management allocates adequate resources (<i>financial, human, etc.</i>) for security improvement.
3. Security Assessment	Risk identification and assessment	Thai (2009), UNCTAD (2006)	Conduct risk identification, using existing data of the organization, as well as other available information about relating risks.
			Conduct risk assessment based on two main elements: probability of an event occurring, and its consequence.
			Use industry standards of risk level for the risk assessment.
	Assessment of the level of compliance with security requirements	Bernard (2009), Rice and Tenney (2007)	Identify and periodically assess the regulations, applicable to the specific shipping organization.
			Identify the list of applicable compulsory and voluntary security requirements.
			Periodically assess compliance with identified security requirements by using internal audits, checklists, as well as external audit, conducted by government or third party for evaluation of compliance with compulsory and voluntary requirements.

	Measures adjustment and investing in security according to risk	Rice and Caniato (2003a), Thai (2009); Sarathy (2006); Sheffi (2008)	Based on the previous steps (components), decide which security measures require more investments and development.
			After necessary changes, conduct security assessment to evaluate the impacts of these changes on organizational performance.
4. Security System, Policy and Procedures	Development of well-structured security policy and procedures and their periodical reviewing	Thai (2009), Williams et al. (2008)	Combine all documents, required by regulations, including those not covered by compulsory documents, and organized them into well-structured security policy.
			Develop the policy based on the features and specification of the organization.
	Business continuity plans and emergency plans and their periodical reviewing	Gould et al. (2010)	Based on risk assessment and identification, develop the various scenarios of security incidents.
			Develop detailed plans for each scenario and review them periodically. Plans have to assure the continuity of organizational operation with any possible security treats.
			Where appropriate, engage business partners for development of the plans.
5. Documentation and Communication	Communication with governments and business partners for security purposes	Thai (2009), Closs, et al. (2008)	Identify which of the security regulations require communication with government.
			Create and maintain reliable network with government, business partners, agents and other parties.
			Identify the details of contact people and develop clear procedures for contacting them.
			Invest in technology, necessary for the security communication.
			Secure communication inside the organization from involvement of inappropriate person.
	Backup communication systems	Russell and Saldanha (2003) in Williams et al. (2008)	Create and periodically amend the backup communication system for the purpose of using it in case of security threats.
	Information security and backups	Rice and Caniato (2003a), Closs, et al. (2008), Thai and Grewal (2007)	Develop and implement procedures to secure all organizational documentation (soft and hard copy).
			Periodically conduct backup of all documentation and information (soft and hard copy).
	Data management	Gutiérrez (2007)	Use international standards for data management.
	IT and financial security	NA	Ensure IT security.
			Ensure financial security.

6. Process Control	Security prevention from the source	Thai (2009), Lee and Whang (2005)	Promote the idea in the organization that security prevention (in-process control) is preferable to final inspection.
			Design all organizational activities to assure prevention of security threats as early as possible, or mitigate them.
			Assure and maintain communication with business partners, if activities or process extended outside the organization.
	Process control and management for security purposes	Thai (2009), ISO (2000, 2005)	Describe in details all organizational processes and activities.
			Assign the personnel responsible for each process or activity in the organization.
			Develop and document the procedure for checking and management of the processes and activities for security purposes.
			Conduct continuous monitoring and review of all processes in the organization.
			Develop and document the detailed procedure for follow-up actions in case if possible security breach is identified.
	Systematic reviewing and improvement of working processes	ISO (2000, 2005), Gould et al. (2010)	Periodical review of all processes and activities in the organization for security, efficiency and resilience purposes.
			If required, introduce necessary changes in the organizational processes.
			Invest in process technologies.
	Creating visibility	Gutiérrez (2007)	Clearly identify all processes and activities in the organization.
			Assure good communication between different participants in the organization (for example, between ashore and offshore personnel).
			Invest in monitoring technologies, such as RFID.
			Develop and/or purchase databases or software for analysis, storage and, where applicable, sharing of the information.
			Develop backup processes.

7. Continuous Security Improvement	Periodical assessment of security management system and its elements	ISO (2000, 2005), Lee and Whang (2005), Thai (2009)	Periodically conduct security assessment by going through the steps of the third factor <i>Security Assessment</i> .
	Correction actions and error cause removal	Bichou, et al. (2007); Sarathy (2006)	Use feedback from employees and customers, audit reports, self-assessment reports, to develop the list of necessary changes in the organizational processes and activities.
			Conduct periodical review and assessment after implementation of proposed changes.
	Research for security purposes	NA	Conduct research and development of security related technologies.
8. Security Incidents Handling and Continuity of Operations	Business continuity plans and emergency plans and their periodical reviewing	Thai (2009); Sarathy (2006)	Identify various scenarios of security threats.
			Develop business continuity and emergency plans for different scenarios and periodically conduct their review.
			Conduct periodical training of employees on implementation of business continuity and emergency plans.
	Recovery plans	Thai (2009)	Develop recovery plans and conduct their periodical review.
			Engage business partners and other parties to work on recovery plans.
	Periodical security and disaster management training	Rice and Caniato (2003a)	Periodically organize security related training and exercises on disaster management.
			Adequately choose the level and type of trainings or exercises to match the type of organization, risks, number of employees and other features.
			Assign the personnel responsible for trainings and exercises in the organization.
9. Business Partners security	Security assessment of business partners	Williams et al. (2008); Sarathy (2006)	Assess future business partners before entering into business relationship with them.
			Periodically assess all current partners to ensure their compliance with security requirements.
			Identify the criteria for assessment of partners. The criteria can include legality, financial solvency and stability, ability to fulfill contractual security requirements, capability to identify and rectify security weaknesses.
			Conduct an assessment of business partners based on the documentation, provided by them.

			When conducting an assessment of business partners, consider their compliance with various voluntary programs (C-TPAT, WCO Framework, ISO standards, STP, etc.).
	Based on previous step, clear distribution of responsibilities (to secure identified gaps) and liabilities between partners	Gujar et al. (2012)	Collaborate with business partners to identify, mitigate and share security risks.
			Clearly define liabilities for possible security incidents in contracts with business partners.
			Clearly define procedures for communication with business partners during security accidents.
	Security trainings and exercises with business partners.	NA	Organize security trainings and exercises jointly with business partners.

Next, hypotheses were developed to answer the second and third research questions, specifically SRQ2.3 about the EMSMM's factors and SRQ3.2 about impacts of the model on organizational performance of shipping companies. Thus, the first hypothesis was formulated as follows:

Hypothesis 1: The activities associated with the following nine groups are essential for the effective management of maritime security in shipping companies: Security Culture; Management and Employee Commitment; Security Assessment; Security Policy, System and Procedures; Documentation and Communication; Process Control; Continuous Security Improvement; Security Incidents Handling and Continuity of Operations; and Business Partners Security.

To answer the third research question about the impacts of maritime security management on organizational performance, the model was evaluated together with categories of organizational performance. According to the discussion in Chapter 2, for the purpose of measuring impacts of the security management, organizational performance of shipping companies are classified into three categories. The process of deriving the categories and their performance indicators was based on the literature review. First, the general literature on organizational performance was reviewed to derive the most commonly used categories. Then the review of literature on performance of shipping companies was conducted and the gaps were identified. Based on the various categorizations of shipping companies' performance for the purpose of measuring impacts of maritime security implementation, three categories and their indicators were proposed, namely *Security Performance*, *Business Resilience* and *Other Business Performance*. The process of deriving the categories is shown in Figure 3.4.

Figure 3.4 Process of deriving categories of organizational performance of shipping companies

The relationships between the model and every category of organizational performance were studied. The impacts of every factor of the model on each category of organizational performance were also tested. Therefore, the second hypothesis in this research is formulated as follows:

Hypothesis 2: The EMSMM positively impacts organizational performance of shipping companies.

Hypothesis 2 is tested through secondary hypotheses:

Hypothesis 2.1: The EMSMM positively impacts security performance of shipping companies:

Hypothesis 2.1.1: Promotion of the Security Culture in shipping companies positively impacts their security performance.

Hypothesis 2.1.2: Management and Employee Commitment positively impacts security performance of shipping companies.

Hypothesis 2.1.3: Security Assessment positively impacts security performance of shipping companies.

Hypothesis 2.1.4: Developed and implemented Security Policy, System and Procedures positively impact security performance of shipping companies.

Hypothesis 2.1.5: Documentation and Communication Security positively impacts security performance of shipping companies.

Hypothesis 2.1.6: Process Control positively impacts security performance of shipping companies.

Hypothesis 2.1.7: Continuous Security Improvement positively impacts security performance of shipping companies.

Hypothesis 2.1.8: Measures for Security Incidents Handling and Continuity of Operations positively impact security performance of shipping companies.

Hypothesis 2.1.9: Business Partners Security positively impacts security performance of shipping companies.

Hypothesis 2.2: The EMSMM positively impacts business resilience of shipping companies.

Hypothesis 2.2.1: Promotion of the Security Culture in shipping companies positively impacts their business resilience.

Hypothesis 2.2.2: Management and Employee Commitment positively impacts business resilience of shipping companies.

Hypothesis 2.2.3: Security Assessment positively impacts business resilience of shipping companies.

Hypothesis 2.2.4: Developed and implemented Security Policy, System and Procedures positively impact business resilience of shipping companies.

Hypothesis 2.2.5: Documentation and Communication Security positively impacts business resilience of shipping companies.

Hypothesis 2.2.6: Process Control positively impacts business resilience of shipping companies.

Hypothesis 2.2.7: Continuous Security Improvement positively impacts business resilience of shipping companies.

Hypothesis 2.2.8: Measures for Security Incidents Handling and Continuity of Operations positively impact business resilience of shipping companies.

Hypothesis 2.2.9: Business Partners Security positively impacts business resilience of shipping companies.

Hypothesis 2.3: The EMSMM positively impacts other business performance of shipping companies.

Hypothesis 2.3.1: Promotion of the Security Culture in shipping companies positively impacts their other business performance.

Hypothesis 2.3.2: Management and Employee Commitment positively impacts other business performance of shipping companies.

Hypothesis 2.3.3: Security Assessment positively impacts other business performance of shipping companies.

Hypothesis 2.3.4: Developed and implemented Security Policy, System and Procedures positively impact other business performance of shipping companies.

Hypothesis 2.3.5: Documentation and Communication Security positively impacts other business performance of shipping companies.

Hypothesis 2.3.6: Process Control positively impacts other business performance of shipping companies.

Hypothesis 2.3.7: Continuous Security Improvement positively impacts other business performance of shipping companies.

Hypothesis 2.3.8: Measures for Security Incidents Handling and Continuity of Operations positively impact other business performance of shipping companies.

Hypothesis 2.3.9: Business Partners Security positively impacts other business performance of shipping companies.

Figure 3.5 shows the hypotheses of this research, including the tested relationship between the model and its factors and categories of organizational performance of shipping companies.

Figure 3.5 Hypotheses tested in this study

3.6. Data Collection Methods

Both qualitative and quantitative methods of data collection are utilized in this study. Data collection for this project was conducted in several stages. To obtain preliminary information, a number of exploratory interviews were first conducted. Based on the results of these interviews, the main questionnaire was designed for the next stage of data collection. To confirm the results of the main survey for Hypothesis 1, a confirmatory survey based on the AHP technique was then conducted.

3.6.1. Exploratory Interviews

The structured interview was applied as a method of data collection to obtain preliminary information. This approach was chosen because of the topic's nature. Since the purpose of conducting the exploratory interviews was to understand the respondents' opinion regarding the proposed model and its factors, as well as to prepare a background for other questions studied in this research, the interviews were conducted using the structured interview form. However, deviations during interviews were necessary to collect some clarifying information.

3.6.1.1. Population and Sampling

Since security is a very sensitive and delicate topic for shipping companies, not many employees possess the necessary information and have access to some security related data. Therefore, the choice of interviewees was done carefully to ensure the obtaining of the greatest possible volume of required information. They were chosen among managers of shipping, ship management and consulting companies who are in charge of risk and security management, such as the company security officer, managers of safety and security departments, designated persons ashore etc. Thus the interviewees are directly involved in the drafting of security management policy for the company.

Thirteen in-depth interviews were conducted within a two-month period, January – March 2013. At that time, all interviewees were permanently based in Singapore and therefore the interviews took place in Singapore. Among these thirteen interviewees, nine were from shipping companies, three from ship management companies, and one from a consulting company focusing on security management. As shown in Table 3.4, three of the interviewees represented a management level, seven – a middle management level and three interviewees held an operational level position. Table 3.5 provides data regarding interviewees’ years of experience in the security related job or industry.

The companies of the interviewees owns or operates various types of vessels, including tankers, bulk carriers, containers, general cargo ships and other types, such as tugs and supply vessels. The profile of the type of vessels in operation is shown in Table 3.6. Their contact details were extracted from the existing databases of Nanyang Technological University. The prospective interviewees were approached through E-mail with a cover letter sent together with an interview information sheet explaining the research background, aims and the method of data collection. The cover letter and the information sheet are shown in Appendices 1.1 and 1.2.

Table 3.4 Interviewees’ designation

Level of position	Number of the interviewees holding the position of the level
Senior management	3
Middle management	7
Operational level	3

Table 3.5 Interviewees' experience in the security related job or industry

Years	Number of the interviewees
0 – 4	5
5 – 9	5
10 – 19	2
20 – 29	1
> 30	0

Table 3.6 Types of vessels owned or operated by the companies of the interviewees

Type of vessels	Number of the companies owning or operating vessels of this type
General cargo ship	1
Containership	3
Bulk carrier	4
Tanker	8
Others	2

3.6.1.2. Interview Form and Procedure

The interview form consists of three parts. The first part contains a series of close-ended and open-ended questions designed to elicit the participants' views regarding the security management system in their companies. The interviewees were asked to indicate their opinion on the implementation of each factor of the EMSMM, as well as on the implementation and effectiveness of various security measures in their companies. The second part includes questions about their companies' organizational performance, including security performance, business resilience and other business performance. Interviewees were asked to indicate if they have observed any significant changes in these categories of organizational performance since the security system was implemented in their companies. The last part of the interview form is designed to solicit the demographic information

regarding the interviewee's organization. Sample of the interview form is provided in Appendix 1.3.

All thirteen interviews were conducted in the interviewees' offices. Seven interviews were audio-recorded, however, other respondents did not allow recording because of security issues. The average interview's length was about one hour. Following the preliminary analysis of the interviews conducted, the EMSMM was revised accordingly. The nine factors were kept without changes, however it was decided to remove the components from the model to reduce its complexity. The attributes were reformulated, as recommended by the interviewees, without changing their meaning. The number of attributes was reduced to 56. The reduction was done by deleting some of the attributes and combining several of them together. The reason for these changes was dictated by the interviewees' opinion regarding the attributes, such as confusion between similar attributes, unnecessary separation of attributes, etc.

3.6.2. Main Survey

3.6.2.1. Population and Sampling

To compose the mailing list for the survey, the Seaweb database was used. This database was chosen because of several reasons. Firstly, Nanyang Technological University has a subscription to it, which allows the students to have full access to the data. Secondly, the Seaweb contains sufficient data on various companies in the shipping industry from all over the world. Thus, the information such as company name, type, location, contact details, etc. can be accessed. Besides that, the database's filters help to choose the necessary companies.

The target population for the survey includes shipping and ship management companies worldwide. To compose the mailing list, the stratified sampling method was used. First, countries were divided according to the world's regions, based on the United Nations country grouping. Then, the information on shipping and ship management companies was extracted for every region. In total, the information about 46,871 shipping and ship management companies was exported from the

database. Among them, Africa was represented by 2,202 companies (4.7%), America – by 5,431 (11.6%), Asia – by 17,572 companies (37.5%), Europe – by 17,757 (37.9%), Middle East – by 2,633 (5.6%), and Oceania – by 1,276 (2.7%). Next, 90% of the sample population was dropped based on the guidelines offered by Gay and Airasian (2003, p.113), cited in Leedy and Ormrod (2005). According to their suggestions, if the population size is 5,000 and more, a sample size of 400 should be adequate. Thus, for the purpose of this research, it was decided that ten percent (10%) of the population size be kept. The remaining 10% of the companies were chosen based on the following criteria: The first criterion was that the company owns or manages the following types of ship: tankers, bulk carriers, general cargo ships, container ships, refrigerated cargo ships. This filter was applied to sort out shipping and ship management companies, which are not operating merchant vessels, in order to fit the scope of this thesis. The second criterion was that the information about the company contains E-mail address. Based on these criteria, a list of 4,687 companies was formed. The percentage of the companies in every world's region was the same as in the total mailing list. Accordingly, the number of the companies for the survey was as follows: Africa – 220, America – 543, Asia – 1757, Europe – 1776, Middle East – 263, and Oceania – 128. The distribution of the companies according to the world's region is shown in Table 3.7.

Table 3.7 Percentage and number of the companies in the mailing list according to the world's regions

World's regions	Percent of the companies in the list, %	Number of companies	
		In the initial list	In the final mailing list
Africa	4.7	2,202	220
America	11.6	5,431	543
Asia	37.5	17,572	1,757
Europe	37.9	17,757	1,776
Middle East	5.6	2,633	263
Oceania	2.7	1,276	128
Total	100	46,871	4,687

3.6.2.2. Design of the Questionnaire

Following the revision after the interviews, a survey questionnaire was designed to further validate the EMSMM (Yang and Wei, 2013). The questionnaire contains three parts. Part A is about the effective maritime security management model for shipping companies. It includes 56 statements divided into nine sections. These sections represent the associated factors of the model. The respondents were asked to indicate their perception of every statement with regards to security management in their companies. The 5-point Likert Scale, where 1 represents “Strongly Disagree” and 5 – “Strongly Agree”, was used in Part A.

Part B studies the impacts of maritime security management on organizational performance of shipping companies. It contains 32 items distributed into three sections: Security Performance, Business Resilience and Other Business Performance. To measure changes in the organizational performance, the 5-point scale was used, where 1 represents “Significantly decrease” and 5 – “Significantly increase”. Besides, the “N/A” option was added for the case, if respondents are not able to give an answer about the indicator. Part C seeks to obtain demographic information, such as the respondent’s designation, number of years in a security related job or industry, type of a company, fleet and, in case of the ship management company, type of management it provides, as well as country of the office location.

The questionnaire was developed as a Word document with option buttons, and was secured from being changed without a password. It contains four pages. An alternative version of the questionnaire was developed online, using the SurveyGizmo platform. Samples of the questionnaires are provided in Appendices 2.4.1 and 2.4.2.

3.6.2.3. Questionnaire Pretesting

It is important to ensure face validity of the measurement items of both parts of the questionnaire, Part A and Part B, since some of the items of the EMSMM, as well as some of the indicators of organizational performance of shipping

companies, were proposed by the authors, but not adopted from the existing literature (Dillman, 2001; Hult et al., 2007). Thus, for this study, the face validity of the items was checked by conducting a pretesting with 20 academics and industry professionals in Singapore. Among them, thirteen had an academic background in maritime studies, in which three were closely related to the field of maritime security. Seven more results were received from industry professionals, whereas two of them were working in security management. Sample of the questionnaire pre-test form is provided in Appendix 2.1.

After conducting the interviews and survey pre-test, the model was further revised by deleting three more attributes based on the comments received during pre-testing. As a result, Part A of the questionnaire contains nine factors and 53 attributes. Table 3.8 shows the changes in the EMSMM according to each steps of model development, as discussed earlier in Sections 3.5 and 3.6.1.2. Table 3.9 presents the attributes associated with each of the model's factors based on the changes done at the stages of conducting the interviews and pre-testing. Part B was kept without any changes. The indicators in every category of Part B are shown in Table 3.10. The indicators were categorized based on the discussion provided in Section 2.4 of Literature Review.

Table 3.8 Number of factors and attributes after each step of model development

Step of Model Development		Number of Factors	Number of Attributes
1	Model Building	9	83
2	Exploratory Interviews	9	56
3	Questionnaire Pre-test	9	53

Table 3.9 Factors and attributes of the EMSMM

Factors	Code	Attributes
1. Security Culture	A1.1	Senior management promotes security as an essential part of every day organizational activity.
	A1.2	Security issues are included in the agendas of scheduled management meetings.
	A1.3	Training seminars and courses on maritime security are conducted <u>for managers</u> .
	A1.4	Security trainings, drills, exercises and seminars are periodically conducted <u>for employees</u> .
	A1.5	Security information is periodically distributed among employees by email, posters, videos, etc.
2. Management and Employee Commitment	A2.1	Security related roles and responsibilities are clearly identified and documented for employees.
	A2.2	The procedures for security related decision making are clearly identified and documented.
	A2.3	Senior management considers security investments as a service quality improvement facilitator.
	A2.4	Senior management allocates adequate resources (<i>financial, human, etc.</i>) for security improvement.
	A2.5	Employees from different levels are involved in processes of security related decision making.
	A2.6	Procedures for employees to report security errors and breaches are established.
	A2.7	A platform for employees to propose necessary changes and possible solutions is established.
	A2.8	Reward & Recognition program is established to motivate employees to provide security feedback.
3. Security Assessment	A3.1	The internal security audit of all activities and departments is periodically conducted.
	A3.2	Security related risks are periodically identified.
	A3.3	Security risk assessment is conducted to derive a risk magnitude.
	A3.4	Risk acceptance levels are established based on risk magnitudes and existing control barriers.
	A3.5	Measures are implemented to mitigate identified risks according to risk acceptance levels.
	A3.6	Investments in security are made according to risk magnitude and risk acceptance levels (<i>investments in security facilities, equipment, manpower, etc.</i>).
	A3.7	<u>All prospective employees</u> periodically go through background screening for security purposes.
	A3.8	A background screening of <u>all current employees</u> is periodically conducted for security purposes.
4. Security Policy, System and Procedures	A4.1	A well-structured security management policy is developed and documented.
	A4.2	Security management policy includes security management system, procedures, plans, etc.
	A4.3	Security policy is included in overall company policy.
	A4.4	Security policy, system, procedures, plans do not contradict with other measures and procedures.
	A4.5	Security measures are integrated into daily activities.

5. Documentation and Communication	A5.1	A communication system is established with authorities, partners, agents, etc. for security purposes.
	A5.2	Detailed procedures for security communication are developed and documented.
	A5.3	Data and processes in the communication system are periodically backed up.
	A5.4	Measures to secure organizational documentation and information are developed and implemented.
	A5.5	Documentation and information systems are periodically backed up.
	A5.6	IT security measures are implemented.
6. Process Control	A6.1	Management promotes the idea of security prevention by making it right from the first time.
	A6.2	A measurement system is developed and put in place to monitor and review all security processes.
	A6.3	A proofreading system is used to detect security loopholes and implement corrections immediately.
	A6.4	Tracking and tracing technologies are implemented for commercial and security purposes.
	A6.5	Procedures for detection and response to security incidents are clearly defined and documented.
	A6.6	Investments in technologies, software and/or equipment are made to improve access control.
7. Continuous Security Improvement	A7.1	Security procedures are constantly reviewed and improved according to security requirements.
	A7.2	Security targets, methods and a time line are clearly established and documented.
	A7.3	Corrective actions and removal of the root cause of security errors are timely undertaken.
	A7.4	We conduct research on security improvement and/or participate in similar projects.
8. Security Incidents Handling and Continuity of Operations	A8.1	We consider and predict all various scenarios of maritime security threats.
	A8.2	Disaster, crisis management and emergency plans are developed based on considered scenarios.
	A8.3	Training and drills on disaster and crisis management are periodically conducted.
	A8.4	Recovery and business continuity plans are developed and reviewed.
	A8.5	Training and drills on recovery and business continuity management are periodically conducted.
	A8.6	Dedicated communication channels exist for emergency cases.
9. Business Partners Security	A9.1	All future business partners undergo security background checks.
	A9.2	All current partners are periodically assessed to ensure their compliance with security requirements.
	A9.3	Security trainings and exercises are jointly organized with business partners.
	A9.4	Collaboration with business partners exists to identify, mitigate and share security risks.
	A9.5	Liabilities for possible security incidents are clearly defined in contracts with business partners.

Table 3.10 Categories of organizational performance of shipping companies and their indicators

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

3.6.2.4. Survey Administration

The administration of the survey was conducted in two steps. To gather information prior to the main survey, in order to improve its quality and effectiveness, a pilot survey was conducted. The target population for the pilot survey consisted of 100 companies located in Singapore. The mailing list included respondents who were earlier approached for the exploratory interviews. The questionnaire was distributed by e-mail. A cover letter was sent together with the

Word document and URL link to the on-line survey. A reminder was sent in two weeks' time. The cover letter and the reminder letter are shown in Appendices 2.2 and 2.3. In total, there were 13 responses for the pilot survey, which gave a response rate of the 13%. Analysis of responses was done using descriptive statistics. After the data analysis, all items were retained in the questionnaire.

After running the pilot survey and analysing the results, the main survey was administrated. Similar to the piloting stage, the questionnaire was distributed by e-mail, together with a cover letter and URL link to the online survey. The cover letter included a description of the research study, aims and the survey deadline. It was sent to the remaining 4,587 companies in the final mailing list. Within two weeks, forty-four completed questionnaires were received. Among them, twenty-three were filled online, twenty one were sent back as a completed word file. Besides, four emails were received saying that the companies did not wish to participate, eleven companies indicated that they are not shipping or ship management companies and were not able to help. Moreover, within two weeks after the survey was sent, 1,021 notices of failed delivery were received.

The first reminder was sent two weeks later. The following companies were excluded from the mailing list: those who had already participated in the survey (if it was possible to track), those who expressed their unwillingness to participate and those who indicated that they were not shipping or ship management companies. However, e-mail addresses, from which the notices of failed delivery were received, were kept in the list. The mailing list for the first reminder included 4,539 companies. Similar to the first survey administration, the reminder was sent by e-mail together with a reminder letter, the link to the online questionnaire and the attached Word file. Within the following two weeks, thirty-eight completed questionnaires were received. Among them, twenty-one were filled online and 17 sent back as the attached Word document. Six companies replied that they were unable to participate because they are not shipping or ship management companies. Nine hundred ninety-eight notices of failed delivery were received.

The second reminder was sent two weeks later after the first reminder. It was sent to 4505 e-mail addresses. This number represents the mailing list after excluding the companies that have responded (if it was possible to track). Within

the following two weeks, twenty-five completed questionnaires were returned, fifteen of them were completed online, and ten were sent back via e-mail. Three companies indicated that they were not interested in participation, and another three replied saying that they are not shipping or ship management companies. 1,002 notices of failed delivery were received.

The final third reminder was sent two weeks later. The questionnaire was sent via e-mail to 4,484 addresses. The data collection was continued for four weeks after the second reminder and then the survey was closed. After the third reminder was sent, eleven more filled questionnaires were received, where four were sent via e-mail and seven were filled online. Besides, three refusals to participate in the survey were received. Notices of failed delivery to 1,007 e-mail addresses were received.

The total sampling population was recalculated after completion of the survey. The initial number (4,687 companies) was reduced by the number of non-shipping or ship management companies ($11+6+3=20$ companies) and by the number of received failed delivery notices (998 companies – the smallest number among the three was used). Thus the final sampling population included 3,669 companies.

3.6.2.5. Response Rate

As indicated in Section 3.6.2.4, the final sampling population included 3,669 companies. The total number of responses, including piloting, first mail-out and reminders, made 131. However several respondents did not answer all of the questions. After a closer examination of the received responses, two questionnaires were withdrawn because of the great amount of missing data in Part A of the questionnaire, resulting in 129 responses. The response rate was low at 3.5%. The low response rate in this research was expected. It may be explained by several reasons. Firstly, the nature of the topic such as security is very sensitive for the managers. That is the reason why majority of companies are not willing to disclose security related information. Secondly, the questionnaire was sent to the general e-mail addresses of shipping and shipping management. Even though the cover letter contained the request to resend the e-mail to the personnel in charge of security

management in the company, it is still highly possible that a big part of the e-mails did not reach the necessary people. Thirdly, it is possible that the length of the questionnaire and the time necessary to filling it up were some of the reasons of low response rate. Even though after pre-testing, the questionnaire was shortened as much as possible, the final version still contained four pages and requires about 15-20 minutes to fill it up. A non-response bias test was performed using ANOVA test to find if there is a significant difference between sets of returned questionnaires. For this purpose, the 129 responses were divided into five groups: piloting, the first mail-out, the first reminder, the second reminder and the third reminder. The results of the ANOVA test showed that at the 5 percent significance level, there were no significant differences between these five groups. The results of the ANOVA test are shown in Appendix 4. Although the response rate was low at 3.5%, the number of 129 responses is sufficient to perform the statistical data analysis.

3.6.2.6. Data Editing, Coding, Categorising and Entry Process

The data in the returned questionnaires was edited and coded to make it ready for the data analysis. Editing is the process necessary to ensure the reliability, completeness and consistency of data (Zikmund, 2003). Upon receiving back the questionnaires, each of them was examined to ensure that there was no missing or multiple answers. Besides, the editing process included looking for inconsistencies between answers to the related questions and reviewing the clarity of the answers for open-ended questions. When any of the discussed problems was found, the respondent was approached again to clarify the necessary information. However, due to the confidentiality issue, it was not always possible to track the respondents when the questionnaire was filled on-line. For those questionnaires, missing answers were highlighted but left without changes.

After editing, the data needs to be coded and entered into the storage file. The coding process is important to prepare the data for being analyzed using necessary statistical software. The process of data coding should be conducted cautiously since human errors are possibly involved. Additionally, the system for coding the answers for the open-ended questions should be designed carefully to reduce the

subjectivity of the given answers. The judgment of the authors should be based on thoughts, and not only on the words of respondents (Zikmund, 2003). For instance, the classifying question about respondent's designation was designed as open-ended. For the analysis of data, the answers were further coded based on the three levels' system: senior management level, middle management level and operational level. The closed-ended questions were coded using numbers (1,2,3, etc.). The answers "N/A" and missing answers were coded as a blank cell. It is important to leave them blank instead of using "0" (zero) because some statistical software (for instance, SPSS) automatically removes the "blank" answer from analysis, whereas zero is considered as a response and used in the analysis.

After editing and coding, the responses were added into an Excel sheet. The variables were categorized and named according to the structure of the questionnaire. The data in the Excel sheet was examined for compliance with the received responses to find and correct mistakes. From the Excel sheet, the data was further entered into SPSS. Later the reversing of the answers, when required, was conducted in SPSS.

As mentioned earlier, two questionnaires were initially withdrawn because of the great amount of missing data in Part A of the questionnaire. After withdrawal, the number of responses became 129. This number of responses was used further for the analysis of the data regarding the EMSMM. In some questionnaires received, Part B contained more missing data than Part A. This result was expected because some of the questions in Part B might be partly out of scope of knowledge of target population. Additionally, the answers "N/A" were further considered as missing data. Thus, after further examination of the received questionnaires, 25 more questionnaires were withdrawn. Therefore, the total number of responses used for the analysis of data describing organizational performance, as well as impacts of the EMSMM on the organizational performance, was 104.

3.6.3. AHP Survey

To confirm the results obtained from the questions asked in Part A of the questionnaire, a confirmatory survey based on the Analytic Hierarchy Process

(AHP) technique was conducted. The purpose of this survey was to rank the factors of the EMSMM based on their importance for security management as perceived by respondents. The AHP method was proposed by Saaty (1977, 1980) and since then was widely used for decision-making process. The method is based on pair-wise comparison of studied factors and, besides identifying the most important alternatives, it also helps to set the priorities (Sato, 2004).

The AHP method has been widely applicable for model development in studies related to supply chain and transportation management. For example, Hwang et al. (2005) applied this technique to develop a supplier selection and planning model. A risk-based maintenance policy selection using AHP was proposed by Arunraj and Maiti (2010). In the context of safety and security management, AHP technique was also used by Chan (2004) for determining priority in a safety management system. Dagkinis and Nikitakos (2013) suggested a strategy to enhance ship safety based on maintenance strategies by applying AHP. Besides, the approach for identifying relative importance of factors to improve passenger security checks at airports, suggested by Kwang and Youn (2006), was based on the AHP methodology. However, this method has not been applied before in studies on maritime security management. In this research, the AHP technique is used to rank the importance of the EMSMM's factors. This ranking might be beneficial for the purpose of making decisions regarding investments in security measures, personnel allocation and general planning of security related activities. The explained methodology is suitable for that purpose, since it helps to create a hierarchy that best suits the main goal of the proposed model, which in this case is an effective management of maritime security.

3.6.3.1. Population and Sampling

Since the purpose of conducting the AHP survey was to confirm and extend the results of the main survey by ranking the model's factors based on their importance for security management as perceived by the main survey's respondents, the mailing list included the email addresses of those who participated in the survey and indicated the willingness to receive the executive summary of the study. Among

129 respondents, 105 indicated their email addresses and therefore composed the mailing list.

3.6.3.2. Design of the AHP Questionnaire

The questionnaire for the AHP survey contains four parts. Section A seeks to explain the factors of the Effective Maritime Security Management Model for Shipping Companies. Besides the description of every factor of the model, their attributes were listed. Section B provides examples of the terms and scales used in this survey. Section C seeks to explore respondents' perception of the relative importance of the selection factors. The two-sided 9-points scale of relative importance is used in the questionnaire, where 1 represents "equal importance" and 9 represents "extreme importance" of one factor to another. The scale of relative importance is shown in Table 3.11. Section D is about respondents' demographic information, such as respondent's designation and trading area of ships operated by respondent's company. The questionnaire, as shown in Appendix 3.2, containing four pages, was developed as a Word document with option buttons, and was secured with a password to prevent changes.

Table 3.11 Scale of relative importance

Intensity of Relative Importance	Definition
1	Equal Importance
2	Equal to Moderate Importance
3	Moderate Importance of one over another
4	Moderate to Strong Importance
5	Essential or Strong Importance
6	Strong to Demonstrated Importance
7	Demonstrated Importance
8	Demonstrated to Extreme Importance
9	Extreme Importance

3.6.3.3. Survey Administration

The questionnaire was distributed via E-mail together with a cover letter. Cover letter is provided in Appendix 3.1. The respondents were asked to return a filled questionnaire within two weeks time. One week after the first mail-out, the follow up email was sent. By the cut-off-date 16 completed questionnaires were received, representing a 15% response rate.

3.6.3.4. Data Editing, Coding, Categorising and Entry Process

One of the steps for applying the AHP, developed by Saaty (1980), is to construct a pair-wise comparison matrix by using the scale of relative importance shown in Table 3.10. For this purpose, the rating data were transferred to the Excel sheets in the form of nxn matrix, where n indicates a number of the model's factors used for comparison. The cells in the matrix show a relative importance of a row factor to a column factor. For example, if the row factor i has equal to moderate importance to the column factor j (in other words, the row factor i is 2 times more important than the column factor j), then the corresponding cell ij contains "2", whereas the cell ji contains "1/2". Using this technique, 16 pair-wise matrices were constructed, according to the number of received responses. Appendix 3.3 shows an example of the matrix.

3.7. Errors and the Ways Used to Reduce Them

The errors in business research are often associated with instrumentation biases and response biases (Hair et al., 2003, Zikmund, 2003). Instrumentation biases are those related to the design of research instruments. To reduce instrumentation bias in this research, the questionnaire was carefully designed and pretested, as discussed earlier in this chapter. Response biases can be connected to the subjectivity of the collected information, misleading of the survey questions or tendency of participants to answer questions in a certain direction (Zikmund, 2003). As discussed in the literature review, the subjectivity may lead to the bias of the information, whereas the bias may result in unreliability of the obtained results

(Boyne, 2006; Dawes, 1999; González-Benito and González-Benito, 2005; Richard, et al., 2009). However, this bias was addressed by using different subjective methods (Boyne, 2006). Richard, et al. (2009) believed that careful questionnaire design and selecting well-informed respondents is essential to ensure the validity of the obtained data and to minimize the errors. Thus to reduce response bias during data collection for this study, the interview form and questionnaire were carefully designed to avoid any type of leading questions or questions that may influence responses in any way. Besides, to ensure that the most reliable information was obtained, the choice of interviewees was done carefully.

Moreover, the errors in the analysis of the survey results are mostly associated with statistical errors and might be caused by low survey response rate. Because of the nature of the topic, a majority of the companies are unwilling to disclose any security related information, which resulted in a very low response rate. However, the number of responses collected for the purpose of this study is enough to conduct data analysis.

3.8. Methods of data analysis

To answer the research questions in this study as well as to test the formulated hypotheses, various methods of data analysis were utilized. As discussed earlier, the secondary data analysis based on the literature review was conducted and the results are presented in Chapter 2. The data collected during the interviews and surveys were analysed as follow.

The qualitative information gathered through the interviews was analysed manually based on the content. The quantitative data collected from the main survey were empirically analysed using the statistical software package SPSS, version 20, including the add-on AMOS. The data collected through the confirmatory survey were analysed by using the AHP technique, as discussed earlier in Section 3.6. Additionally, for some of the answers to the open-ended questions where coding was not possible, the thematic analysis based on the content was applied.

3.9. Summary

In this chapter, the research questions, research aims and objectives and hypotheses were presented. The chapter provided a detailed explanation of how the proposed model was developed, it also introduced the model's factors, their components and associated attributes. Some of the factors were partly derived from the existing models and frameworks for security management, while others were developed based on the principles of the management approaches commonly used for security management. Moreover, the existing compulsory and voluntary requirements for shipping companies were taken in consideration at every step of the literature review and model development. The changes in the model's factors and the associated attributes were further introduced based on results of the interviews and the questionnaire's pre-testing. Apart from the presentation of the tested relationship, three categories of organizational performance were introduced. The methods of data collection, such as exploratory interviews and two type of survey, were then discussed, including a detailed information about sampling population, design of the instruments and administration. The chapter also explained potential errors and the ways in which these errors were addressed in the study. Finally, it discussed the methods of data analysis utilised in this research.

CHAPTER 4. EFFECTIVE MARITIME SECURITY MANAGEMENT IN SHIPPING COMPANIES

4.1. Introduction

This is the first chapter of two providing analysis and interpretation of the findings in this study. This chapter presents the results of the in-depth interviews and survey with a purpose to validate the EMSMM proposed in this research. Firstly, a selection of statistical techniques used for data analysis is described, followed by the discussion on respondents' profile, including their designation, professional experience, as well as business sector and trading area of the respondents' companies, etc. The validation of the proposed model is presented next. It includes the discussion on the implementation and effectiveness of security requirements in the participants' companies, which helps in answering one of the sub-questions of the first research question, SRQ1.3. The validation of the model's factors is conducted based on the results of the interviews and the main survey. To rank the importance of the factors, the results of the AHP survey are analysed. Thus, this chapter provides conclusions to the second research question and the first hypothesis in this study. The chapter ends with the summary of the findings and discussion on the EMSMM and its factors.

4.2. Statistical Techniques for Data Analysis

To answer the second research question in this study, various methods of data analysis were utilized. The qualitative information gathered through the interviews was analysed manually based on the content. The quantitative data collected from the survey were empirically analysed using the statistical software package SPSS, version 20, including the add-on AMOS. Additionally, for some of the answers to the open-ended questions where coding was not possible, the thematic analysis based on the content was applied.

To analyse the quantitative data collected during the survey, several statistical methods were used. Firstly, descriptive statistical analysis was conducted to demonstrate the respondents' profile based on the classifying information. Furthermore, to validate the EMSMM and its factors, the exploratory factor analysis (EFA) was conducted in SPSS. Later the model was analysed in AMOS by conducting the confirmatory factor analysis (CFA). The final version of the model was then tested for reliability and validity issues. The difference in perception of the model by participants was also studied based on their designation and trading area of their companies.

Factor analyses were utilized in this study, since the proposed model and the composed scale of performance indicators have not been tested before. Therefore, it was important to determine the number and the nature of possible factors and to understand their influence on their attributes. A combination of the EFA and CFA was used, since it is believed that "EFA may be appropriate for scale development while CFA would be preferred where measurement models have a well-developed underlying theory for hypothesized patterns of loadings" (Hurley et al., 1997, p. 668). Thus, the EFA was used to bring intercorrelated variables together and to determine the number of latent factors, and resulted in the output, which could be used for a further statistical analysis (Field, 2000; Rietveld and Van Hout, 1993). An overview of steps of the EFA is shown in Figure 4.1. Next, the CFA was conducted to confirm the determined factors and their attributes. The CFA usually deals with a measurement model and the relationship between its dependent and independent variables. The purpose of the CFA is to determine how well the attributes describe their factor.

Figure 4.1 An overview of the steps in an exploratory factor analysis
Source: Rietveld and Van Hout (1993, p. 291)

Then, to rank the model's factors confirmed by EFA and CFA, the AHP technique was utilized. To analyze the data received from the AHP survey, the methodology proposed by Saaty (1980) was used. The analysis using the AHP method is usually conducted in several steps. Firstly, the problem and decision-making criteria are identified. Then the data are collected from respondents by using a pair-wise comparison. Based on that, matrices of pair-wise comparison are constructed for every response. The maximum eigenvalue $\lambda_{\max}$ and the corresponding normalised right eigenvector (the priority vector) of the comparison

matrices are then calculated, followed by evaluation of the consistency of the matrices. For this purpose, the consistency index, C.I., is calculated as

$$C.I. = (\lambda_{\max} - n)/(n - 1).$$

The consistency ratio (C.R.) is then calculated as a ratio C.I./R.I., where R.I., a random matrix, is taken from the book of Saaty (2009). The consistency ratio is used to check whether the decision-maker's comparisons were consistent or not. The value of C.R. less than or equal to 0.1 corresponds to the desirable consistency of the matrix. If C.R. is between 0.1 and 0.2, the consistency is considered as acceptable (Saaty, 1980, 200, 2009). The acceptance of the matrices with C.R. less than 0.2 was widely supported by researchers in different areas (Byun, 2001; Lee and Walsh, 2011; Karlsson and Ryan, 1997; Kim et al., 2010; Kim et al., 2012; Park and Kim, 2014). The priority vector shows the judged importance of the model's factors. The described process is shown in Figure 4.2.

Figure 4.2 An overview of the steps of the AHP used in this study

Even though the AHP is widely applicable by academics and in industry sectors, it also has its limitations. The most often discussed limitation is related to the rank reversal. “Rank reversal means that the rank of an alternative resulting from AHP may change when another alternative is added to the initial group of alternatives compared” (Hartwich, 1999, p.14). However, according to Saathy (1980), introduction of new alternatives in the existing model results in a new model with a new ranking received after conducting the AHP analysis. In this research the model containing six factors were analysed by using the AHP and there was no intention to introduce any other alternatives.

The second limitation, a scale limitation, is related to a choice between the use of verbal comparisons and numerical ones. Some authors are concerned about the language ambiguity when using a verbal comparison (Donegan et al (1992) in Ishizaka and Labib, 2009), whereas others believe that preferences cannot be assessed using the numerical scale, because an absolute zero does not exist (Barzilai (2005) in Ishizaka and Labib, 2009). Based on the recommendations of Saathy (1977, 1980), in this research a verbal scale was converted into a numerical one, as shown in Table 3.11, and presented in the questionnaire (see Appendix 3.2).

The possible inconsistency resulted from a large number of comparisons may become a reason for another limitation of the AHP (Hossain et al., 2014). A large number of comparisons may burden the experts, after some time they might lose interest (Hartwich, 1999). In this study this possible limitation was addressed by avoiding using a large number of comparisons. As can be seen from Appendix 3.2, fifteen comparisons were used to collect the data in the AHP survey.

Finally, the AHP analysis does not account for the interrelationships among the attributes (Palcic and Lalic, 2009). However, in this study this limitation would not have a significant impact on the results, since the compared attributes are important factors of the EMSMM and they supposed to be implemented simultaneously. The results of the AHP in this research should provide a ranking of the factors, which is important for managers to prioritise the implemented measures.

4.3. Respondents Profile

Several demographic variables were used in the survey to collect the information about survey participants and their companies. The information about respondents includes their designation and years of professional experience:

- *Designation of the respondents*: this variable was coded in three categories, namely, senior management level, middle management level positions, and operational level.
- *Number of years in the security related job or industry*: this variable was coded in the following categories: 0-4 years, 5-9 years, 10-19 years, 20-29 years, 30 years and above.

The information about respondents' companies was represented in the questionnaire by the following variables:

- *Business Sector*: this variable was pre-coded in the questionnaire with three classified groups, namely, shipping company, ship management company, and others.
- *Types of ships in operation*: this variable was pre-coded in the questionnaire to further elaborate the information on shipping and ship management companies. There were several categories used, namely general cargo ship, container ship, tanker, bulk carrier, and other.
- *Trading area*: similar to the previous variable, this variable was used to elaborate more on the shipping or ship management company. It was pre-coded into eight categories, with consideration of the United Nations country grouping of World's regions. The categories were named as follows: Worldwide, Asia, Europe, Middle East, Africa, North America, South America, and Oceania.
- *Type of management provided by the company*: this variable was used when the respondent chose ship management company as the company's business sector. This variable was pre-coded into four categories as follows: technical management, crew management, commercial management, and others.
- *Location of the office*: this variable was coded after the questionnaire was returned into seven categories, according to the United Nations country grouping of

World's regions, namely Asia, Europe, Middle East, Africa, North America, South America, and Oceania.

The profile of respondents and their employing companies based on the discussed demographic variables is presented in Figures 4.3 to 4.9. Some of the questions about classifying information allowed single entry only and others gave a possibility to choose multiple answers.

Figure 4.3 Respondents' designation

Figure 4.4 Respondents' experience in the security related job or industry

Figure 4.5 Respondents' business sector

Figure 4.6 Location of the respondents' offices

Figure 4.7 Types of ships in operation of the respondents' companies

Figure 4.8 Types of management provided by the respondents' companies

Figure 4.9 Trading area of the respondents' companies

4.4. Perception of the EMSMM in Shipping Companies

As discussed in Chapter 3, the validation of the proposed EMSMM was conducted through in-depth interviews and surveys. The results are presented in this section. The section is organized as follows. Firstly, to provide a background for the topic, the general view on maritime security management (MSM) in shipping companies is discussed. Next, the information about implementation and effectiveness of various security requirements in participating companies is given. Finally, the validation of the EMSMM is conducted.

4.4.1. General View on Maritime Security Management (MSM) in Shipping Companies

The participants' opinions on the MSM were quite diverse. Some of them believed that compulsory security requirements play an important role in security management practice. Others, who were more concerned about security, argued that shipping companies had already implemented security measures even before they became mandatory. One of the respondents commented as follows:

From a practitioner's view, security regulations haven't brought big differences for us in the industry world. The practice onboard the ship hasn't changed significantly... Generally, the regulations gave us some framework for the work we had been doing before.

Some participants believed that the compulsory nature of security requirements increased the awareness in their companies. However, in their opinion, the increased awareness is the only positive impact of compulsory requirements, such as the requirements of the ISPS Code. To ensure security in a shipping company, the company needs to apply its own security measures and develop its own management system. This perception was further elaborated by one of the participants who commented that "security very much depends on the level of commitment. A good owner would provide additional security measures when necessary."

Thus, in some participating companies the voluntary requirements were implemented even before their participation in government programs. Therefore, the changes of security measures for the certification purposes were not very significant and did not require big investments. However, some participants indicated that they had to manage some problems related to the lack of common procedure when implementing different voluntary security programs. Although several programs have mutual recognitions of one another's certification, a majority of them require separate certification. This is illustrated in one of the comments as follows:

The main thing with these programs is that too many programs are coming up and they all have sort of the same requirements... They are quite close, only elements change... We would like to see more mutual recognitions between programs – it's much easier.

Moreover, the security management system in a company significantly depends on its trading. The US region was found the most troublesome in terms of restrictions and requirements:

We have to spend time and money to go to US ports... There are a lot of various procedures required for ship to do before going to US... And if we don't know them we're in big problems.

Therefore, all of the participants agreed upon the need for a common regulatory framework or model which helps in security management. Besides, there were also different opinions regarding the structure of the security management systems in companies. Some companies have management systems containing a number of 'Standards' describing in detail all security related procedures and activities in the company. The security policies in these companies are not limited by requirements of the ISPS Code. Industry standards are also considered as minimum requirements. In some other companies, policies are very brief and mostly focused on mandatory requirements and documentation:

We consider security policies as guidance. That's why we believe they should be brief, just like a statement that is easy to remember. However, after providing the policy we also provide the explanation and training to employees.

The examples above show that even though the participating companies implement the same security requirements, their implementation approaches are quite diversified. Some companies simply focus on the implementation of compulsory security measures, others are actively participating in various voluntary programs. The discussion on the implementation of various single security requirements is provided next.

4.4.2. The Implementation of Security Requirements in Shipping Companies

The first research question of this study was partly answered in the literature review chapter. The lists of maritime security regulations and requirements were provided in Tables 2.1, 2.2 and 2.3. Further, to answer the SRQ1.3, it was studied which of the listed requirements are implemented in the participating companies. It was observed that these companies have implemented the majority of the listed compulsory and voluntary requirements. However, a number of measures were found not implemented. For example, one of the companies did not conduct routine checking of cargo, but left this duty to other participants of the supply chain. It was explained by the company's good faith relationship with its business partners, as well as by strict procedures for choosing and assessing the partners. Moreover, it was found that some of the participating companies did not use Seafarers' Identity Documents. It was commented that these companies implemented their own identification documents because of convenience.

Participants also identified some security measures implemented in their companies apart from the listed requirements, for example, a tracking system, armed guards on board, citadels and safe master points on board a ship with secure control, navigation and communication systems, contingency plans for ships, and other anti-piracy measures such as using binocular vision devices, search lines, bubble wires, bullet-proof helmets, jackets and visors, etc. All of them indicated that their companies followed the recommendations of IMO Best Management Practice and, if necessary, IMO Guidance on the use of privately contracted armed security personnel on board of their ships. Moreover, one of the participating companies conducted research on the development of an independent tracking

system, which can continue to operate when the power on board is cut off. One of the companies even went far beyond the general practice of security management: jointly with the government, port operators and other business partners, they proposed and developed security incident scenarios that have not been considered before as a possibility for maritime security threats and conducted training and exercises based on those scenarios. Thus, it can be concluded that the list of maritime security requirements implemented in shipping companies varies significantly. Compulsory requirements are mostly implemented in full, whereas implementation of voluntary requirements depends on the company's management system.

4.4.3. Validation of the EMSMM

This section investigates the general perception of the EMSMM's factors by interviewees and survey's respondents. To explore and validate the structure of the EMSMM, the exploratory factor analysis (EFA) was conducted, followed by the confirmatory factor analysis (CFA). EFA was performed to explore the factor structure of the proposed model. The first run of the EFA on 53 measurement items revealed that the strength of inter-correlations was good. The Kaiser-Meyer-Olkin (KMO) index is 0.874, which is greater than the suggested minimum of 0.60 (Hair at al., 1995), and Barlett's test of sphericity ($p = 0.000$) indicated the stability of the EFA. The analysis was run based on the principle components method and Varimax rotation technique. The first run resulted in ten components with eigenvalues above 1, explaining 73.49% of the variances. Also, a rotated component matrix was produced as a result of the analysis.

Next several runs of the EFA were conducted using the commonly accepted procedure for decision-making, where "an item is loaded highly on one factor (i.e. more than 0.5) and lowly on all other factors" (Thai, 2013, p. 123). Following this procedure, those items not loaded highly enough on one factor or highly loaded on several factors, were dropped one by one. The decision to drop an item was also done based on the item's significance on the meaning of its corresponding factor. It

was carefully examined if the dropping would jeopardize the content of the factor. In total, 22 items were dropped during the EFA process.

The analysis on the remaining 31 items revealed that KMO measure of sampling adequacy (0.884) and the value of Barlett's test of sphericity ($p = 0.000$) still met the standards (Table 4.1). This run resulted in six factors explaining 72.447% of variances, in that Factor 1 explains 42.127% of variances, 11.477% of variances were explained by Factor 2, 5.608% by Factor 3, 5.191% by Factor 4, 4.15% by Factor 5, and 3.894% by Factor 6 respectively, as shown in Table 4.2. Besides, Table 4.2 also shows the component rotated matrix generated as a result of the last run of EFA.

Table 4.1 KMO and Bartlett's Test – last run of factor analysis

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy		0.884
Bartlett's Test of Sphericity	Approx. Chi-Square	2547.849
	Df	465
	Sig.	0.000

As can be seen from Table 4.2, all items are loaded highly (i.e. more than 0.50) into one factor only, and there is no item loaded highly on several factors. Subsequently, the EFA was conducted for every factor of the new model to ensure that the items of each factor are not spread out into more factors. The results supported the existence of only six factors. Factor 1 consists of ten items A3.8, A6.4, A6.6, A7.4, A8.5, A9.1, A9.2, A9.3, A9.4, and A9.5. The majority of these items explain the security relationship with business partners, therefore the name of this factor is kept as *Business Partners Security* (PARTNER). Factor 2 only contains items of *Security Policy, System and Procedures* (PROCED) in the proposed EMSMM, namely A4.1, A4.2, A4.3, A4.4, and A4.5. Thus, the same name was given for this factor. Meanwhile, there are four items loaded highly on Factor 3, namely A5.3, A5.4, A5.5, and A5.6. Since all of these items represent the factor of *Documentation and Communication* (DOCUM), the original name was

used. Factor 4 consists of three items of A8.2, A8.3, and A8.6. All these items are with *Security Incidents Handling and Continuity of Operations* (INCID) in the original model and therefore the factor retains its original name. Factor 5 includes items of A1.2, A1.4, A1.5, A2.1, and A2.6. These items represent two factors in the original model, namely, *Security Culture* and *Management and Employee Commitment*. However, as they mostly focus on the contribution from managers and employees and reflect their commitment in security management, for the purpose of the study a new factor including these items was named *Management and Employee Commitment* (COMIT). The last Factor 6 consists of four items namely A3.3, A3.4, A3.5, and A3.6. These items represent the factor of *Security Assessment* (ASSES) in the original model, and thus this factor takes its original name.

To further validate the resulted six-factor structure of the EMSMM constructed from the EFA, the CFA was performed using AMOS 20. 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, including A1.2, A1.4, A1.5, A3.6, A3.8, A6.4, A6.6, A7.4, and A8.5. The decision to drop an item was also done based on its significance on the meaning of its corresponding factor. For example, the withdrawal of items A3.8, A6.4, A6.6, A7.4 and A8.5 from the factor of *Business Partners Security* (PARTNER) resulted in the same structure of the factor, as it had in the original model. Therefore, the withdrawal did not impact the meaning significantly. For the factor of *Management and Employee Commitment* (COMIT), the dropping of items A1.2, A1.4 and A1.5 resulted in only two items left in the factor. However, these two items fully represent the meaning of the factor. Figure 4.10 shows the EMSMM based on the CFA.

Table 4.2 EFA with Varimax rotation results

Measurement items	Factors					
	1	2	3	4	5	6
A9.2	0.865	0.246	0.122	0.075	0.132	0.033
A9.5	0.848	0.104	-0.036	0.224	-0.059	0.154
A9.1	0.840	0.043	0.155	-0.050	0.190	0.048
A9.3	0.816	0.032	0.081	0.212	0.145	0.108
A9.4	0.778	-0.049	0.223	0.282	0.109	0.146
A3.8	0.723	0.215	0.067	-0.138	0.126	0.125
A6.4	0.679	0.193	0.234	-0.188	0.133	0.209
A7.4	0.667	0.156	0.204	0.028	0.195	0.081
A8.5	0.626	0.233	0.131	0.363	0.028	0.164
A6.6	0.570	0.24	0.368	-0.153	0.208	0.283
A4.2	0.142	0.813	0.232	0.226	0.185	0.042
A4.4	0.314	0.762	-0.005	0.062	0.107	0.115
A4.3	0.132	0.757	0.305	0.266	-0.004	0.254
A4.1	0.173	0.724	0.292	0.132	0.200	0.242
A4.5	0.177	0.533	0.342	0.109	0.335	0.305
A5.4	0.264	0.293	0.756	0.225	0.061	0.139
A5.6	0.218	0.119	0.731	0.199	0.229	0.221
A5.5	0.193	0.304	0.702	0.253	0.152	0.183
A5.3	0.237	0.236	0.625	0.194	0.382	-0.006
A8.3	0.111	0.134	0.250	0.794	0.130	0.169
A8.2	0.146	0.151	0.431	0.695	0.190	0.164
A8.6	-0.097	0.248	0.168	0.667	0.195	0.165
A1.5	0.199	-0.021	0.226	-0.064	0.798	0.116
A1.4	0.243	0.237	0.031	0.248	0.683	0.012
A2.1	0.090	0.324	0.179	0.405	0.626	0.193
A2.6	0.122	0.254	0.097	0.468	0.617	0.067
A1.2	0.167	0.071	0.292	0.085	0.603	0.379
A3.4	0.292	0.287	0.209	0.189	0.136	0.776
A3.5	0.257	0.355	0.146	0.147	0.154	0.758
A3.3	0.128	0.069	0.392	0.296	0.234	0.606
A3.6	0.314	0.120	-0.048	0.500	0.074	0.551
Eigenvalue	13.059	3.558	1.739	1.609	1.287	1.207
Variance explained (%)	42.127	11.477	5.608	5.191	4.150	3.894
Cumulative variance (%)	42.127	53.603	59.212	64.403	68.553	72.447

Figure 4.10 The EMSMM resulted from the CFA

The EMSMM resulted from the CFA contains 22 measurable items and has the model fit characteristics meeting the suggested standards proposed by Bollen (1989), and Hair et al. (2010). Specifically, the minimum discrepancy/degree of freedom (CMIN/DF) should be less than 3.0 (good level), comparative fit index (CFI) should be greater than 0.90 (good level), root mean square error of approximation (RMSEA) should be smaller than 0.05 (good level) or smaller than 0.10 (moderate level), root mean square residual (RMR) should be as small as possible towards 0. In this study, the last run of CFA resulted in the following model fit characteristics: CMIN/DF = 1.934, RMR = 0.037, CFI = 0.918, GFI = 0.808, NFI = 0.846 and RMSEA = 0.085. Therefore, the six factors and 22 items contribute to a good level of the overall fit of the EMSMM and confirm the results of the EFA.

The descriptive statistics data regarding perceptions of attributes and factors of the EMSMM by survey respondents, including their ranks, mean and standard deviation, are shown in Tables 4.3 and 4.4, respectively. It can be seen from the Table 4.3 that the majority of attributes have a low value of standard deviation (lower than 1), which means that the variability of individual observation from the mean score is not high. However, some attributes of the factor *Business Partners Security* (PARTNER) (A9.1, A9.2, A9.3) have standard deviation value above 1. That shows some disagreement between respondents about this factor. This disagreement was also notable during interviews. Specifically, some of the participating companies limit the procedures in this area with a basic security check before signing a contract with a new contractor, whereas others have detailed approved procedures for the assessment of current and prospective partners. However, it was observed that more and more attention is paid to this area of security management recently. Another factor, which was perceived differently by participants, is *Documentation and Communication Security* (DOCUM). Some companies paid more attention to this factor, whereas others implemented it on the very basic level and believed that it is not very important for security purposes.

Table 4.3 Perceptions of the attributes of the EMSMM's factors

Attributes of the EMSMM's factors		Rank	Mean	Std. Dev.
A2.1	Security related roles and responsibilities are clearly identified and documented for employees.	1	4.36	0.71
A4.3	Security policy is included in overall company policy.	2	4.33	0.76
A8.6	Dedicated communication channels exist for emergency cases.	3	4.28	0.73
A4.2	Security management policy includes security management system, procedures, plans, etc.	4	4.26	0.72
A2.6	Procedures for employees to report security errors and breaches are established.	5	4.22	0.65
A3.5	Measures are implemented to mitigate identified risks according to risk acceptance levels.	6	4.21	0.74
A4.1	A well-structured security management policy is developed and documented.	7	4.20	0.72
A8.2	Disaster, crisis management and emergency plans are developed based on considered scenarios.	8	4.16	0.70
A3.3	Security risk assessment is conducted to derive a risk magnitude.	9	4.13	0.76
A8.3	Training and drills on disaster and crisis management are periodically conducted.	10	4.12	0.78
A3.4	Risk acceptance levels are established based on risk magnitudes and existing control barriers.	11	4.10	0.79
A5.6	IT security measures are implemented.	12	4.10	0.76
A4.4	Security policy, system, procedures, plans do not contradict with other measures and procedures.	13	4.07	0.83
A5.4	Measures to secure organizational documentation and information are developed and implemented.	14	4.05	0.66
A5.5	Documentation and information systems are periodically backed up.	15	4.05	0.74
A4.5	Security measures are integrated into daily activities.	16	3.99	0.84
A5.3	Data and processes in the communication system are periodically backed up.	17	3.95	0.83
A9.4	Collaboration with business partners exists to identify, mitigate and share security risks.	18	3.57	0.93
A9.5	Liabilities for possible security incidents are clearly defined in contracts with business partners.	19	3.50	0.93
A9.3	Security trainings and exercises are jointly organized with business partners.	20	3.47	1.09
A9.2	All current partners are periodically assessed to ensure their compliance with security requirements.	21	3.31	1.07
A9.1	All future business partners undergo security background checks.	22	3.26	1.06

Notes: relative ranking based on attributes' mean scores; 1 = strongly disagree, 5 = strongly agree.

Table 4.4 Perceptions of the factors of the EMSMM

Factors of the EMSMM		Rank	Mean	Std. Dev.
COMMIT	Management and Employee Commitment	1	4.29	0.62
INCID	Security Incidents Handling and Continuity of Operations	2	4.19	0.64
PROCED	Security Policy, System and Procedures	3	4.17	0.65
ASSES	Security Assessment	4	4.14	0.68
DOCUM	Documentation and Communication	5	4.04	0.64
PARTNER	Business Partners Security	6	3.42	0.90

Notes: relative ranking based on attributes' mean scores; 1 = strongly disagree, 5 = strongly agree.

The results of the statistical analyses are supported by those of the interviews. It was found that, generally, all factors of the EMSMM are implemented and included in the security management systems of participating companies. It was observed that much attention is paid to some factors such as *Security Incidents Handling and Continuity of Operations* (INCID), *Management and Employee Commitment* (COMIT), *Security Assessment* (ASSES) and *Security Policy, System and Procedures* (PROCED). In this aspect, one of the respondents believed that “everything starts with the security assessment... the policies and other components of security management are developed based on the assessment’s results.” Besides, one of the interviewees mentioned that *Management and Employee Commitment* (COMIT) is a widely implemented factor in his company. It is expressed by a “single point of the accountability’s rule”, which means that the employee responsible for security issues has to make sure that others will be involved if it is necessary. This approach has shown its effectiveness during security incident trainings and exercises in the company, as well as when the real incidents have taken place. However, another company does not pay so much attention to this factor. The interviewee mentioned that “very seldom, employees are penalized when the security rules violations are observed”.

Nevertheless, all participants agreed that human factor is the utmost important element in security management and that every company’s security management system should be based on employees. One of the participants expressed the opinion that “the most difficult part of security management is to change people and culture.” That means those factors of the model, which contain the human factor,

such as *Management and Employee Commitment (COMIT)*, *Security Policy, System and Procedures (PROCED)*, and *Security Incident Handling and Continuity of Operations (INCID)*, should be strongly emphasised. Table 4.5 shows how many out of thirteen interviewed companies constantly exercised each factor of the model at the time of the interview, while already considering them as important. It also indicates how many companies considered it to be not so important for security improvement and thus did not exercise it at all.

Table 4.5 Profile of the interviewed companies with regard to implementation and importance of the model's factors

Factors	Number of interviewed companies that	
	implemented the factor	considered the factor as not important for security improvement
Management and Employee Commitment	5	2
Security Assessment	5	0
Security Policy, System and Procedures	7	0
Documentation and Communication	6	3
Security Incidents Handling and Continuity of Operations	7	1
Business Partners Security	2	2

It can be concluded that although not every factor of the proposed EMSMM was considered equally important and implemented for security improvement in the participating companies, they are still perceived by the participants as necessary factors of a holistic security management model. The model was strongly supported by all participants, with a high emphasis on the importance of a systematic approach to security management.

4.5. Measurement Validity and Reliability Analysis

Further, the EMSMM was examined for validity and reliability. The results, as shown in Table 4.6, confirm that the model has no validity concerns. The characteristics describing convergent and discriminant validity as well as composite

reliability (CR) meet the suggested requirements (Fornell and Larcker, 1981; Hair at al., 2010). Specifically, CR should be greater than 0.7 and average variance extracted (AVE) is greater than 0.5, whereas CR should be bigger than EVA. Meanwhile, maximum shared squared variance (MSV) and average shared squared variance (ASV) smaller than AVE confirms the discriminant validity. It can therefore be concluded that the model resulted from the CFA is valid and reliable.

Table 4.6 Results of the validity and reliability test in CFA

Factors	CR	AVE	MSV	ASV
INCID	0.869	0.691	0.554	0.346
PARTNER	0.927	0.719	0.202	0.160
PROCED	0.900	0.644	0.511	0.390
DOCUM	0.894	0.680	0.410	0.346
COMMIT	0.770	0.627	0.554	0.398
ASSES	0.891	0.733	0.462	0.352

Besides, the model was also analysed for scale reliability. The scale reliability analysis was conducted in SPSS. Firstly, the scale reliability analysis was conducted for the whole scale and included 22 measurement items. Cronbach's Alpha of 0.939 proved a very reliable level of the scale (Cronbach's Alpha > 0.8). Next, the reliability was examined according to the factors of the model. Table 4.7 shows that all factors of the model are reliable (Cronbach's Alpha > 0.7) or very reliable (Cronbach's Alpha > 0.8). Besides, Corrected Item-Total Correlation for all items is above 0.5.

Table 4.7 Reliability Statistics and Item-Total Statistics for factors of the EMSMM

Factor	Cronbach's Alpha	Items	Corrected Item-Total Correlation
COMMIT	0.783	A21	0.646
		A26	0.646
ASSES	0.867	A33	0.634
		A34	0.860
		A35	0.758
PROCED	0.893	A41	0.804
		A42	0.809
		A43	0.806
		A44	0.633
		A45	0.668
DOCUM	0.883	A53	0.689
		A54	0.807
		A55	0.804
		A56	0.707
INCID	0.844	A82	0.757
		A83	0.763
		A86	0.621
PARTNER	0.930	A91	0.778
		A92	0.841
		A93	0.828
		A94	0.830
		A95	0.809

4.6. Perception of the EMSMM's Factors based on the Respondents' Designation and Trading Areas of Their Companies

In order to examine whether there are significant differences between groups of respondents' designations and trading areas of their companies, the ANOVA tests were performed at 95% and 99% confidence levels. The respondents were divided into four groups according to their designation, namely *Senior level*, *Middle level*, *Executive level*, and those who did not indicate their designation. For the purpose of examining the respondents perception based on the trading area of their companies, the companies were divided into three groups: those with multiple-region trading area, with single region trading area, and unknown area. Tables 4.8 and 4.9 show that, for all factors of the model, the significance values of the test are all greater than 0.05, and thus indicating that there is no significant difference between the groups of respondents' designations and trading areas of their companies in relation to the factors of the EMSMM. However, it can be seen from these tables that the results are quite mixed. Some factors (*Management and Employee Commitment*, *Security Policy*, *System and Procedures*, and *Business Partners Security*) are less agreed by respondents of different designation levels or from companies with different trading areas, and some (*Security Assessment*, *Security Incidents Handling and Continuity of Operations*, and *Documentation and Communication*) have a higher level of consensus from the survey participants.

Table 4.8 Perception of the EMSMM's factors based on respondents' designation

Factor	Designation	Mean	STDV	Sig
COMMIT	Senior level	4.481	0.574	0.230
	Middle level	4.204	0.630	
	Executive level	4.333	0.577	
	Not indicated	4.500	0.577	
ASSES	Senior level	4.244	0.643	0.573
	Middle level	4.082	0.707	
	Executive level	4.333	0.577	
	Not indicated	4.417	0.500	
PROCED	Senior level	4.295	0.746	0.543
	Middle level	4.105	0.604	
	Executive level	4.333	0.577	
	Not indicated	4.350	0.854	
DOCUM	Senior level	4.202	0.557	0.178
	Middle level	3.944	0.662	
	Executive level	4.333	0.577	
	Not indicated	4.375	0.750	
INCID	Senior level	4.256	0.648	0.816
	Middle level	4.145	0.644	
	Executive level	4.333	0.577	
	Not indicated	4.333	0.816	
PARTNER	Senior level	3.477	0.736	0.325
	Middle level	3.346	0.947	
	Executive level	4.000	1.000	
	Not indicated	4.000	0.849	

Notes: analyses performed at 95% and 99% confidence levels.

Table 4.9 Perception of the EMSMM's factors based on the trading area

Factor	Trading Area	Mean	STDV	Sig
COMMIT	Multiple-region	4.329	0.608	0.596
	Single region	4.188	0.704	
	Not indicated	4.214	0.393	
ASSES	Multiple-region	4.197	0.693	0.443
	Single region	4.028	0.728	
	Not indicated	3.962	0.133	
PROCED	Multiple-region	4.223	0.671	0.330
	Single region	4.086	0.632	
	Not indicated	3.886	0.324	
DOCUM	Multiple-region	4.075	0.709	0.622
	Single region	3.958	0.509	
	Not indicated	3.893	0.197	
INCID	Multiple-region	4.215	0.663	0.677
	Single region	4.153	0.629	
	Not indicated	4.000	0.509	
PARTNER	Multiple-region	3.499	0.917	0.187
	Single region	3.133	0.915	
	Not indicated	3.626	0.384	

Notes: analyses performed at 95% and 99% confidence levels.

4.7. Relative Importance of the Factors of the EMSMM: Perception of the Nine Experts

The remaining six factors of the model, namely *Management and Employee Commitment* (COMIT), *Security Policy, System and Procedures* (PROCED), *Security Assessment* (ASSES), *Documentation and Communication* (DOCUM), *Security Incidents Handling and Continuity of Operations* (INCID), and *Business Partners Security* (PARTNER), were further analyzed by applying the AHP methodology. This analysis was conducted to explore and prioritize the importance of the model's factors for effective security management.

The data collected during the confirmatory survey was transformed to Excel sheets and analyzed as described in the methodology chapter of this thesis. For all sixteen matrices, the priority vector was calculated. The priority vector contains

weights of the factors and shows the judged importance of every factor. To evaluate the matrix consistency, the consistency ratio (C.R.) was then calculated as a ratio of consistency index (C.I.) to a random index (R.I.), C.I./R.I. Whereas C.I. is calculated as

$$C.I. = (\lambda_{\max} - n)/(n - 1),$$

where $\lambda_{\max}$ is the maximum eigenvalue of the judgement matrix. R.I. is taken from the book of Saaty (2009). For the pair-wise comparison matrix with six compared parameters, R.I. is 1.25.

The matrix is consistent when value of C.R. is less than 0.2 (Saaty, 1980, 2000, 2009). Among sixteen matrices, seven were not consistent, since their C.R. was greater than 0.2. Therefore, nine out of sixteen responses were used for the further data analysis. Among them six matrices had a desirable consistency level (C.R. is less than or equal to 0.1) and three – acceptable level (C.R. is between 0.1 and 0.2). According to Vargas (2001), when the AHP is used for a group decision making, it is appropriate to use an average C.R. for evaluating consistency of the responses. The average C.R. of the nine matrices is 0.09, which corresponds to the desirable level of consistency. The consistency ratios of the nine matrices are shown in Appendix 3.4.

The data collected from these nine respondents were enough to conduct the AHP analysis in this research. According to Saaty and Özdemir (2015, p. 9), the number of judges does not matter, however it is important to select “judges that have both knowledge and practical experience with the matter”. In this research, the respondents satisfy both conditions. Either they hold a top-management position in their company or they are involved in security management. Among nine experts, two were holding a position of vice president of the companies, two were technical managers, two – HSE (health, safety and environmental) managers, and three of the respondents were CSOs (company security officers). Therefore, it is believed that their experience and knowledge are at the required level and it is appropriate to conduct the analysis based on their responses.

To examine the importance of every model’s factor resulted from the second survey, the weight of each factor was calculated as a geometric average of the factor’s weights resulted from each of nine matrices. The harmonized weights,

percentages and ranking of the factors are shown in Table 4.10. Harmonized weights for each of nine matrices are provided in Appendix 3.4. The graphical representation is given in Figure 4.11.

Table 4.10 Factors' weights resulted from AHP analysis

Factors		Rank	Harmonized Weights, Geometric Average	Percentage, %
COMMIT	Management and Employee Commitment	1	0.17	20
INCID	Security Incidents Handling and Continuity of Operations	2	0.16	19
PROCED	Security Policy, System and Procedures	3	0.15	18
ASSES	Security Assessment	4	0.14	16
DOCUM	Documentation and Communication	5	0.12	14
PARTNERS	Business Partners Security	6	0.11	13

Figure 4.11 Importance of the EMSMM's factors

The results of the AHP analysis provide information on the importance of the model's factors, which is essential for the managers when they develop and implement a security management system in their companies. The ranking highlights the areas of the security management, which require more attention. The results of the AHP analysis support the results of statistical analysis shown in Table 4.4. As can be seen from Tables 4.4 and 4.10, the most important factor of the EMSMM is *Management and Employee Commitment* (COMIT; 20%), followed by *Security Incidents Handling and Continuity of Operations* (INCID; 19%) and *Security Policy, System and Procedures* (PROCED; 18%). The least important factors are *Business Partners Security* (PARTNER; 13%), *Documentation and Communication* (DOCUM; 14%), and *Security Assessment* (ASSES; 16%). However, comparatively small difference between percentages of the most and the least important factors (20% and 13%, respectively) indicates, that all of factors are considered quite important for security improvement.

4.8. Discussion

In this chapter the EMSMM, its factors and associated attributes were tested through the EFA, CFA and the AHP analysis. The EFA and CFA resulted in six factors of the model and 22 associated attributes. Further, the factors were prioritized according to their importance for security improvement by conducting the AHP analysis based on the data collected from nine experts. Table 4.11 shows the model's factors structured according to their importance, as well as their associated attributes.

Table 4.11 The factors of the EMSMM distributed according their importance and attributes, as resulted from the analyses

Factors of the EMSMM (presented according to their importance)	Attributes
Management and Employee Commitment	Security related roles and responsibilities are clearly identified and documented for employees.
	Procedures for employees to report security errors and breaches are established.
Security Incidents Handling and Continuity of Operations	Disaster, crisis management and emergency plans are developed based on considered scenarios.
	Training and drills on disaster and crisis management are periodically conducted.
	Dedicated communication channels exist for emergency cases.
Security Policy, System and Procedures	A well-structured security management policy is developed and documented.
	Security management policy includes security management system, procedures, plans, etc.
	Security policy is included in overall company policy.
	Security policy, system, procedures, plans do not contradict with other measures and procedures.
	Security measures are integrated into daily activities.
Security Assessment	Security risk assessment is conducted to derive a risk magnitude.
	Risk acceptance levels are established based on risk magnitudes and existing control barriers.
	Measures are implemented to mitigate identified risks according to risk acceptance levels.
Documentation and Communication	Data and processes in the communication system are periodically backed up.
	Measures to secure organizational documentation and information are developed and implemented.
	Documentation and information systems are periodically backed up.
	IT security measures are implemented.
Business Partners Security	Collaboration with business partners exists to identify, mitigate and share security risks.
	Liabilities for possible security incidents are clearly defined in contracts with business partners.
	Security trainings and exercises are jointly organized with business partners.
	All current partners are periodically assessed to ensure their compliance with security requirements.
	All future business partners undergo security background checks.

The ranking of the model's factors after the EFA and CFA was provided in Table 4.4. The results of the AHP analysis were shown in Table 4.10 and Figure 4.9. As can be seen from these tables and the figure, the high concern is currently given to the areas of management, which focus on reducing human errors. Specifically, *Management and Employee Commitment* is essential to involve everybody in a company into security management and increase security awareness. This factor was ranked by respondents as the most important. One of the interviewees commented that the security management "starts with the management and goes down to the staff" and it is necessary "to ensure that everybody is always committed" and "concerned about security". To achieve the total commitment to security in the company it is important to identify and clearly explain employees their security related roles and responsibilities, to ensure that everybody in the company is aware about actions to be taken in case of security incidents and about necessity to report these accidents.

In this respect, the factor of *Management and Employee Commitment* is closely related to the factors of *Security Policy, System and Procedures* and *Security Incidents Handling and Continuity of Operations*. These two factors provide measures for employees, which help them to reduce mistakes and establish preventive measures in different areas of operations. The idea behind these factors is, first, to develop, clearly define and document necessary measures and procedures for security purposes, and second, to convey them to the employees through periodical communication and trainings. This idea is supported by the interviewees. One of them commented that "the policies should be easily understandable, they need to make sense and suit to the company". The interviewees also agreed that the security procedures and measures are more effective when they are implemented in a form of drills, exercises and other communication with the company's staff, including "dissemination of the information, which is bought from databases, sending out the bulletins, training".

Additionally, it is important that these measures and procedures are developed based on the constant security assessment to address the existing risks and prevent possible security incidents. The factor of *Security Assessment*, which was ranked as the fourth important factor, has always been an essential element of security

management system. One of the interviewees expressed the following opinion about security assessment in his company:

Everything starts with security assessment. The policies are developed based on the assessment's results. Since we consider a ship as an extension of an office, the security assessment should be done at both locations. Security assessment is the first thing we do when the accident happens.

Some of the interviewees explained that the risk assessment is periodically conducted in their companies. Additionally, they assess risks when a trading area of their vessels is changed. According to the interviewees' opinion, it is important that corresponding security measures are timely implemented to reduce the possibility of the accident's occurrence or its consequences.

Other approaches to manage the risks include risk avoidance and risk sharing. To avoid the defined risks, it is important to ensure security of *Documentation and Communication*. For that purpose, access to the information and communication channels should be secured, IT security should be maintained and periodical back-ups should be conducted. For instance, in one of the companies, the measures to ensure documentation and communication security are implemented as follows:

Access to the documents is limited to a certain number of people. Communication with authorities is also reported and secured. Master always has communication channels. We also have back-ups in place.

Besides, the evaluated risks can be managed by sharing them with business partners. The factor of *Business Partners Security* was ranked as the least important for an effective security management, even though it is widely implemented in shipping companies. Many of the companies have a strict procedure for choosing their business partners. It is supported by the following comment:

Our suppliers can be only chosen from the approved list of suppliers. Before that they go through the strict control.

Generally, the results show that the factor of *Business Partners Security* is increasingly implemented in the shipping industry. It means that shipping companies nowadays understand the importance and benefits of working with reliable partners. Indeed, to make the whole supply chain more secured, every company in the chain should extend its security management beyond their boundary

at least to its direct partners. However, the opinion was shared that the security improvement is not the main purpose of the collaboration. That is the possible reason for not considering the measures of this factor as very important from the perspective of security improvement.

4.9. Summary

The analysis and discussion in this chapter were presented to answer the first and the second research questions and test empirically the first hypothesis of the study that the effective maritime security management in shipping companies is based on activities associated with nine groups. The data collected through in-depth interviews and two surveys were analysed statistically using SPSS software and AHP technique as well as by applying the thematic analysis.

The findings from the data analysis in this chapter are as follows. Firstly, the results of interviews revealed that among the list of maritime security requirements, the compulsory requirements are implemented almost in full, whereas the implementation of the voluntary requirements depends on the company's management system. Some of the companies even implement requirements in addition to those in the list. These results provide an answer to the sub-research question 1.3 *“What maritime security requirements are implemented in shipping companies?”*

Secondly, the sub-research question 2.4 *“What are the factors of the EMSMM?”* was answered. The analysis of the interviews' and survey's results showed that the EMSMM for shipping companies contains six factors and 22 attributes. These findings suggest that shipping companies wishing to improve security in a more effective way should focus on six main areas of security management: *Management and Employee Commitment, Security Assessment, Security Policy, System and Procedures, Documentation and Communication, Security Incidents Handling and Continuity of Operations*, and *Business Partners Security*. Besides, the validity test of the model confirmed that there are no validity and reliability concerns. Moreover, it is important to highlight that there is no

significant difference in the perception of the proposed model based on the position of the respondents and trading area of the companies.

Thirdly, the importance of the model's factors was ranked using the AHP technique. The results supported the results of the main survey, where *Management and Employee Commitment* (COMIT) was ranked as the most important factor of the EMSMM, followed by *Security Incidents Handling and Continuity of Operations* (INCID) and *Security Policy, System and Procedures* (PROCED). The factor of *Security Assessment* (ASSES) was placed as the fourth important factor of the model, whereas the factors of *Documentation and Communication* (DOCUM) and *Business Partners Security* (PARTNER) were ranked as the two least important.

Generally, it was observed the distribution of the factors was more or less equal, which shows that all of the discussed areas of security management are important for the effective security management and security improvement. The most attention however is currently given to the areas of management focusing on possibility to reduce human errors, such as *Management and Employee Commitment* and *Security Incidents Handling and Continuity of Operations*. Besides, it was observed that the relationship with business partners plays an important role in security management in shipping companies, although the main purpose of implementation of the related measures is not a security improvement.

The results of the analyses presented in the chapter are shown in Table 4.11. The table shows six factors of the model distributed according to their importance and 22 associated attributes. According to these results, the activities associated with the following nine groups are essential for the effective management of maritime security in shipping companies: *Management and Employee Commitment*; *Security Incidents Handling and Continuity of Operations*; *Security Policy, System and Procedures*; *Security Assessment*; *Documentation and Communication*; and *Business Partners Security*, which contributes to a partial support of the first main hypothesis of the study. To manage maritime security effectively, it is recommended to implement all factors of the proposed model simultaneously. The importance of the factors can be prioritised as shown earlier in Table 4.11.

After ranking the importance of the model's factors, it is important to understand their effectiveness with regards to organizational performance of shipping companies, specifically security performance, business resilience and other business performance. Therefore, the next chapter presents an analysis of the impacts of the proposed EMSMM and its factors on various categories of organizational performance of the companies that participated in the main survey.

CHAPTER 5. IMPACTS OF MARITIME SECURITY MANAGEMENT ON ORGANIZATIONAL PERFORMANCE OF SHIPPING COMPANIES

5.1. Introduction

This is the second chapter of two that provide analysis and interpretation of the findings in this study. This chapter presents the results of the information collected through in-depth interviews and survey with respect to the impacts of the model, validated in the previous chapter, to the organizational performance of shipping companies. This chapter aims to answer the third research question of the study and test the second main hypothesis. The chapter is structured as follows. Firstly, a short overview of statistical techniques applied for data analysis is provided. Then, to clarify on the categories of organizational performance of shipping companies proposed based on the literature review, the statistical analysis of data, collected through survey, is conducted. The next two sections discuss a common method bias in the structural model and a way to deal with it, as well as construct the validity and reliability of the model. The second hypothesis's testing is provided next. It is based on the statistical analysis of the information collected through the survey. The discussion on the results is then presented, followed by a brief summary.

5.2. Statistical Techniques for Data Analysis

To answer the third research question of the study, a combination of statistical analysis and thematic analysis is applied. To validate the categories of organizational performance of shipping companies, the data collected through the survey were analysed statistically by conducting an exploratory factor analysis (EFA) in SPSS version 20 and confirmatory factor analysis (CFA) in AMOS. The EFA was conducted to ensure that the proposed structure of categories of organizational performance is valid, and the CFA was conducted to confirm that the indicators explain their respective categories. According to the explanation of the EFA and CFA, provided in Section 4.2 of this thesis, it was also necessary to use

these analyses since the used scale of the performance indicators was composed by the author of the thesis and has not been tested before.

Next, to test the impacts of the model's factors on organizational performance of shipping companies, the model resulted from the EFA and CFA and the categories of organizational performance were analysed together. The analysis was conducted using the Structural Equation Modeling (SEM). This method allows analyzing the links between different elements of the structural model, such as the EMSMM's factors and categories of organizational performance, it provides a possibility to model complex dependencies. In the literature, the SEM is defined as follows:

- SEM is a comprehensive statistical approach to testing hypotheses about relations among observed and latent variables (Hoyle, 1995).
- SEM is a methodology for representing, estimating, and testing a theoretical network of (mostly) linear relations between variables (Rigdon, 1998).
- SEM tests hypothesized patterns of directional and nondirectional relationships among a set of observed (measured) and unobserved (latent) variables (MacCallum & Austin, 2000).

According to Recker (2011), SEM includes validation the measurement model, which is often conducted through CFA, and fitting the structural model through path analysis. Usually this process involves five stages (Recker, 2011), as shown in Figure 5.1:

- Model specification – is an initial specification of the model, where the constructs and links are given based on a previous analysis or research;
- Model identification – “deals with obtaining a unique solution for the model”, such as factor loading, path coefficients or explained variance;
- Model estimation – deals with estimation of the unknown parameters;
- Model fit testing – is a conducting some so-called goodness-of-fit tests to determine how well the estimated model fits;
- Model re-specification – aims to improve model fit characteristics by adding, changing or deleting paths in the model.

Figure 5.1 Stages of the SEM

The SEM was performed using the AMOS add-on. The structural model was also tested for validity and reliability. Finally, the thematic analysis of the information collected through in-depth interviews was applied to reaffirm the results of statistical analysis.

5.3. Relationship between Implementation of the EMSMM and Organizational Performance

5.3.1. Categories of Organizational Performance

To test the relationship between the model's factors and categories of organizational performance of shipping companies, the categories of organizational

performance were first validated through the EFA, followed by the CFA. The EFA analysis was run based on the principle components methods and Varimax rotation technique. The first run of the EFA on 32 measurement items resulted in six factors with eigenvalues above 1.

A rotated component matrix was produced as a result of the analysis. However, the commonly accepted practice suggests that an item should be dropped if it is not loaded highly enough on one factor (i.e. more than 0.5) or highly loaded on several factors (Thai, 2013). Besides, when deciding if the item should be dropped, the significance of the item for the meaning of the corresponding factor was carefully examined. Based on these requirements, during subsequent several runs of the EFA eight items were dropped one by one, namely, B1.8, B1.9, B2.4, B3.1, B3.5, B3.11, B3.12, and B3.13.

The analysis of the remaining 24 items revealed a good strength of inter-correlations. Specifically, the Kaiser-Meyer-Olkin (KMO) index is 0.758, which is greater than the required level of 0.60 (Hair et al., 1995), and Bartlett's test of sphericity ($p = 0.000$) confirms the stability of the EFA (Table 5.1). As a result of the last run, six factors explain 71.156% of variances, in that Factor 1 explains 22.580% of variances, Factor 2 – 19.419%, Factor 3 – 10.951%, 6.970% of variances are explained by Factor 4, 6.533% - by Factor 5, and 4.702% – by Factor 6, as shown in Table 5.2.

Table 5.1 KMO and Bartlett's Test – last run of factor analysis

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.758
Bartlett's Test of Sphericity	Approx. Chi-Square	1508.889
	Df	276
	Sig.	0.000

Table 5.2 EFA with Varimax rotation results

Measurement items	Factors					
	1	2	3	4	5	6
B1.5	0.814	0.192	-0.051	0.007	0.048	0.007
B1.3	0.792	-0.011	0.094	0.000	-0.032	0.056
B1.6	0.772	-0.053	0.021	0.012	0.108	0.117
B1.2	0.762	0.019	0.198	-0.153	0.003	0.140
B1.7	0.724	0.062	0.026	0.142	0.120	0.014
B1.1	0.710	0.062	-0.125	-0.114	0.253	-0.078
B1.4	0.686	0.238	-0.037	0.071	0.233	0.036
B3.17	0.279	0.879	-0.013	0.019	-0.030	0.056
B3.16	0.259	0.858	0.019	-0.036	-0.026	0.110
B3.19	-0.098	0.774	0.024	0.318	0.114	-0.079
B3.15	0.182	0.765	-0.081	0.103	0.077	0.040
B3.18	-0.051	0.750	0.003	0.387	-0.007	-0.068
B3.14	-0.101	0.749	-0.116	-0.125	-0.103	-0.202
B2.2	0.030	-0.036	0.971	-0.041	0.053	0.006
B2.3	0.037	-0.034	0.946	-0.042	0.041	0.088
B2.1	0.035	-0.072	0.924	-0.148	0.052	0.013
B3.2	-0.022	-0.030	-0.018	0.807	0.044	-0.085
B3.3	0.144	0.390	-0.216	0.653	0.017	-0.115
B3.4	-0.042	0.431	-0.136	0.595	-0.130	-0.236
B3.10	0.124	0.020	0.071	0.180	0.824	0.128
B3.8	0.250	0.055	-0.040	-0.019	0.757	0.290
B3.9	0.223	-0.123	0.199	-0.354	0.648	-0.161
B3.7	0.017	-0.031	0.007	-0.061	0.147	0.832
B3.6	0.172	-0.060	0.089	-0.209	0.067	0.784
Eigenvalue	5.419	4.661	2.628	1.673	1.568	1.128
Variance explained (%)	22.580	19.419	10.951	6.970	6.533	4.702
Cumulative variance (%)	22.580	42.000	52.951	59.921	66.454	71.156

As can be seen from Table 5.2, all measurement items are highly loaded in their factors, and none of the items is loaded highly on several factors. The items of organizational performance are distributed into six factors. Factor 1 consists of items B1.1, B1.2, B1.3, B1.4, B1.5, B1.6, and B1.7. These items explain the security performance of shipping companies, and therefore the name of the factor is kept as *Security Performance* (SECURITY). Items B2.1, B2.2 and B2.3 represent the factor of *Business Resilience* (RESILIENCE), and thus this factor takes its original name. The measurement items of the initial category of other business performance are distributed into four factors. Items B3.2, B3.3 and B3.4 form the third factor and describe performance of companies related to reputation and competitive position. According to Table 2.10 in Chapter 2, these performance indicators belong to the category of *Market Performance*, therefore this name is given to the third factor (MARKET). Factor 4 contains items B3.6 and B3.7, which explain the time related performance. Thus, the factor is called *Time Performance* (TIME). Factor 5 consists of three items B3.8, B3.9 and B3.10. These items represent performance indicators, which are related to security performance; however, they do not describe security performance directly and therefore cannot be included into the factor of *Security Performance*. Instead, the factor is named *Security Related Performance* (SECRELAT). The last factor contains items describing the relationship with customers, namely B3.14, B3.15, B3.16, B3.17, B3.18 and B3.19. Hence, the factor is named *Customer Performance* (CUSTOMER).

To further validate the structure of the components of organizational performance, the CFA was performed using AMOS 20. The analysis was run several times to achieve the best model-fit characteristics. As a result, two more items B3.2 and B3.14 were withdrawn to improve validity and reliability of the measurement model. The decision to withdraw the items was justified by their low loadings. Besides, the meanings of the items and their corresponding factors were carefully considered. It was decided to drop these items, since their dropping did not change the semantic meaning of the factors they belong to. Figure 5.2 shows the six factors and measurement items.

Figure 5.2 Categories of organizational performance resulted from the CFA

The CFA of organizational performance resulted in the model fit parameters, which meet the suggested requirements proposed by Bollen (1989) and Hair et al. (2010). 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 contribute to a good model fit and support the results of the EFA.

The 22 indicators were distributed among the categories as following: *Security Performance* included indicators, associated with security incidents, namely: cargo pilferage, stowaways, ship attacks (including terrorist and piracy attack, armed robbery), tampering with cargo, data and physical shipment, cargo loss and damage, smuggling and violations of security rules by employees. The indicators of the category of *Business Resilience* include time taken to identify, mitigate security problems and recover from security incidents. The former category of *Other Business Performance* was distributed into four categories. The category of *Market Performance* is represented by two indicators, namely “level of competitiveness” and “level of reputation for liability”. The indicators “vessels’ port turnaround time” and “total voyage time” explain the category of *Time Performance*. The category *Security Related Performance* of contains indicators such as “number of vessels’ schedule delays because of security issues”, “number of Port State Control inspections” and “additional cost because of security issues”. The category of *Customer Performance* includes five performance indicators, namely flexibility in responding to customer requests, customers’ overall satisfaction about physical resources, customers’ overall satisfaction about quality of service provided, and number of new and repeated customers.

As can be seen from Figure 5.2, the coefficients between some of the independent variables are significantly high. Thus, positive relationship exists between the following variables: MARKET and CUSTOMER (0.47), SECURITY and SECRELATED (0.44), SECRELATED and TIME (0.43), MARKET and TIME (0.37); and SECURITY and CUSTOMER (0.36). It means that there is a possibility that the categories of business performance represented by these variables can affect each other.

The model was then examined for validity and reliability concerns. The results show that the validity and reliability characteristics meet the suggested requirements (Fornell and Larcker, 1981; Hair et al., 2010), and therefore, the model has no validity concerns. As can be seen from Table 5.3, for all six factors of

organizational performance, the composite reliability (CR) is greater than 0.7 and average variance extracted (AVE) is greater than 0.5. Besides, CR is bigger than AVE, whereas maximum shared squared variance (MSV) and average shared squared variance (ASV) are smaller than AVE. Therefore, the model resulted from the CFA is considered as valid and reliable.

Table 5.3 Results of the validity concern check for organizational performance

Factor	CR	AVE	MSV	ASV	Cronbach's Alpha
SECRELAT	0.776	0.541	0.197	0.084	0.691
SECURITY	0.883	0.519	0.197	0.079	0.881
RESILIENCE	0.956	0.878	0.080	0.023	0.955
MARKET	0.772	0.629	0.225	0.092	0.771
TIME	0.718	0.560	0.188	0.081	0.648
CUSTOMER	0.889	0.623	0.225	0.074	0.897

Notes: Significant at $p < 0.05$.

5.3.2. Common Method Bias

The structural model containing six independent factors of the EMSMM and six dependent factors of organizational performance was then constructed. Because a single survey was used to collect data for both dependent and independent variables in this study, it is recommended to test for common method bias (Lowry et al., 2013, Podsakoff et al., 2003). For this purpose, the latent factor method, proposed by Podsakoff et al. (2003), was used to retrieve the common variance. Specifically, the unmeasured common latent factor (CLF) was added to the measurement model. 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 results showed that some of the variables of the factor of *Documentation and Communication* are due to common method bias. Therefore, to control the bias, the CLF was retained in the model. The data were then imputed

from AMOS to SPSS. Further, the imputed data were used to create a structural model with independent and dependent observed variables in SEM.

5.3.3. Construct Validity and Reliability

The measurement model was also tested for reliability and validity issues. The CFA was used to establish construct validity (Churchill, 1991). The loadings of all measurement items on their respective factors were used to calculate important parameters. The results, as shown in Table 5.4, confirm that the measurement model has no validity and reliability concerns, since the parameters are within recommended limits (Fornell and Larcker, 1981; Hair et al., 2010). Specifically, CR is greater than 0.7 and bigger than AVE for all factors of the structural model, whereas the values of AVE are greater than the required minimum of 0.5 and bigger than values of MSV and ASV. Reliability of the factors was also evaluated through the Cronbach's Alfa (Blunch, 2013). The Cronbach's Alfa values of the measurement model's factors are above 0.60, which is considered reliable (Hair et al., 2006).

Table 5.4 Results of the validity and reliability test

	CR	AVE	MSV	ASV	Cronbach's Alpha
COMMIT	0.787	0.649	0.563	0.190	0.783
SECURITY	0.883	0.520	0.192	0.085	0.881
RESILIENCE	0.956	0.879	0.078	0.015	0.955
MARKET	0.772	0.629	0.228	0.053	0.771
TIME	0.721	0.565	0.184	0.040	0.648
SECRELAT	0.776	0.542	0.192	0.060	0.691
CUSTOMER	0.885	0.616	0.228	0.078	0.897
PROCED	0.902	0.650	0.483	0.208	0.893
PARTNER	0.926	0.715	0.247	0.115	0.930
INCID	0.850	0.658	0.563	0.172	0.844
DOCUM	0.891	0.673	0.483	0.197	0.883
ASSES	0.883	0.719	0.413	0.172	0.867

Notes: Significant at $p < 0.05$.

5.3.4. Hypotheses Testing

The first run of the structural equation modeling (SEM) was conducted to test the relationship between all independent and all dependent variables, according to the hypotheses. As mentioned earlier in Section 5.3.2, to avoid common method bias, the variables were imputed from the model in AMOS, which included CLF. The model fit test revealed a necessity for a model re-specification. According to Recker (2011) model re-specification is one of the stages of the SEM process, which aims to improve model fit characteristics. Deleting (insignificant) paths and adding or changing paths in the model are the forms of model re-specification. However, for a model re-specification stage “it is important that the modifications also make theoretical sense” (Recker, 2011, p.106).

The first run of the SEM showed that some paths between variables were not significant. Therefore, it was decided to delete 26 paths with a standardized path coefficient below 0.15, namely: COMMIT → SECURITY, COMMIT → TIME, COMMIT → SECRELAT, COMMIT → CUSTOMER, ASSES → SECURITY, ASSES → RESILIENCE, ASSES → MARKET, ASSES → SECRELAT, ASSES → CUSTOMER, PROCED → RESILIENCE, PROCED → MARKET, PROCED → SECRELAT, DOCUM → SECURITY, DOCUM → RESILIENCE, DOCUM → MARKET, DOCUM → SECRELAT, DOCUM → CUSTOMER, INCID → SECURITY, INCID → RESILIENCE, INCID → MARKET, INCID → SECRELAT, INCID → CUSTOMER, PARTNER → RESILIENCE, PARTNER → MARKET, PARTNER → TIME, and PARTNER → SECRELAT.

Before deleting each of the listed paths, it was carefully considered if this change makes any theoretical sense. The main argument for the consideration was based on the understanding, that often a sole implementation of one factor of the model would not affect any business performance. However, since all factors are related with each other, a direct relationship on specific category of business performance might be clearly visible only for one of the factors. Besides, the relationships of the model's factors on the category of *Business Resilience* are insignificant or the significance is low, since a majority of the responding companies did not experience real cases where business resilience was threatened,

and therefore they were only able to indicate the changes of this performance based on the trainings and exercises. This limitation will be discussed further in section 6.4 of the thesis.

It was also observed that significant relationships exist between some dependent variables. Specifically, two dependent variables, namely SECRELAT and MARKET, had no significant relationship with any of the independent variables. However, the significant relationships existed between dependent variables SECURITY and SECRELAT as well as between CUSTOMER und MARKET. Thence, it was decided to test the relationships between independent variables and dependent variables SECRELAT and MARKET using the mediator variables SECURITY and CUSTOMER respectively. These changes were also justified based on the content of these categories. Thus, the category *Security Related Performance* includes three indicators, namely *Vessels' schedule delays because of security issues*, *Number of Port State Control inspections on the company's vessels* and *Additional cost because of security issues*. It would be logical to assume, that this performance changes analogically to *Security Performance*. Likewise, the category of *Market Performance* contains indicators such as *Level of competitiveness* and *Level of reputation for liability*. These indicators are closely related to the category of *Customer Performance* and are therefore affected by the model's factors through this category.

After the discussed changes another run of the SEM was conducted. The final version after conducting the SEM is shown in Figure 5.3. It has the model fit characteristics within the acceptable range: 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. Thus, the overall model fit contributes to the adequacy of the model.

Figure 5.3 Results of the main SEM model 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; significant at $p < 0.05$.

The hypothesized relationships were tested using the associated standardized regression coefficient of the paths. Table 5.5 shows results of hypothesis testing. It can be seen that PROCED has a significant positive impact on SECURITY ($\beta=0.385$), therefore, *H2.1.4* 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 *H2.1.9* and *H2.2.2* are also supported. The link between COMMIT and TIME ($\beta=0.915$) is also significant, implying the partial support of *H2.3.2*. The hypothesis is supported partially, since only one among four categories of *Other Organizational Performance* is positively impacted. Similarly, *H2.3.5* and *H2.3.9* are supported partially, since only one category among four is impacted positively. Specifically, DOCUM positively impacts TIME ($\beta=0.516$), and the relationship between PARTNER and CUSTOMER are also positive ($\beta=0.220$). *H2.3.4* is not supported, since together with positive relationship on CUSTOMER ($\beta=0.269$), PROCED has a negative link on TIME ($\beta=-0.434$). *H2.3.3* is also not supported, because the significant negative relationship between ASSES and TIME was found ($\beta=-0.238$). Similarly, negative impact of INCID on TIME ($\beta=-0.578$) implies that *H2.3.8* is not supported.

Thus, the results of the analysis, as shown in Figure 5.3 and Table 5.5, proves that the measures associated with *Business Partners Security* and *Security Policy, System and Procedures* improve security and consequently security related performance of shipping companies. These measures include the following: A well-structured security management policy is developed and documented, Security management policy includes security management system, procedures, plans, etc., Security policy is included in overall company policy, Security policy, system, procedures, plans do not contradict with other measures and procedures, Security measures are integrated into daily activities, All future business partners undergo security background checks, All current partners are periodically assessed to ensure their compliance with security requirements, Security trainings and exercises are jointly organized with business partners, Collaboration with business partners exists to identify, mitigate and share security risks, and Liabilities for possible security incidents are clearly defined in contracts with business partners. By implementing

the listed measures the companies participating in the survey were able to improve security performance related to cargo pilferage, stowaways, ship attacks (including terrorist and piracy attack, armed robbery), tampering with cargo, data and physical shipment, cargo loss and damage, smuggling and violations of security rules by employees, as well as to reduce vessels' schedule delays because of security issues, number of Port State Control inspections and an additional cost because of security issues.

Besides, implementation of the listed security measures has other proven benefits. The participants of the survey have observed improvement in the *Customer Performance*, specifically the following indicators have been improved: flexibility in responding to customer request, customers' overall satisfaction about physical resources, their overall satisfaction about quality of service provided, number of new and repeated customers.

Other factors of the proposed model have not shown a proven influence on security performance, however the results demonstrate their impacts on other business performance of the participating companies. Thus, the security measure associated with *Management and Employee Commitment*, such as Security related roles and responsibilities are clearly identified and documented for employees, and Procedures for employees to report security errors and breaches are established, have improved resilience and time performance indicators, namely, time taken to identify security problems, to mitigate security problems and recover from security incidents, as well as vessels' port turnaround and total voyage time.

The time performance has been also positively impacted by the measures related to the *Documentation and Communication Security*, such as Data and processes in the communication system are periodically backed up, Measures to secure organizational documentation and information are developed and implemented, Documentation and information systems are periodically backed up, and IT security measures are implemented. However, the negative impacts on time performance were also observed in the participating companies. Specifically, the following measures increase vessels' port turnaround and total voyage time: A well-structured security management policy is developed and documented, Security management policy includes security management system, procedures, plans, etc.,

Security policy is included in overall company policy, Security policy, system, procedures, plans do not contradict with other measures and procedures, Security measures are integrated into daily activities, Security risk assessment is conducted to derive a risk magnitude, Risk acceptance levels are established based on risk magnitudes and existing control barriers, Measures are implemented to mitigate identified risks according to risk acceptance levels, Disaster, crisis management and emergency plans are developed based on considered scenarios, Training and drills on disaster and crisis management are periodically conducted, and Dedicated communication channels exist for emergency cases. These negative impacts on time performance can be associated with extra responsibilities and paperwork required from a ship crew. Besides, it is important to consider the fact, that all model's factors should be implemented together to achieve positive results. To demonstrate this fact a further analysis was conducted.

Table 5.5 Results of relationship testing between the EMSMM's factors and organizational performance

Paths			Hypotheses	Standardized path coefficients	Results
SECURITY	<---	PROCED	<i>H2.1.4</i>	0.385	Supported
SECURITY	<---	PARTNER	<i>H2.1.9</i>	0.151	Supported
RESILIENCE	<---	COMMIT	<i>H2.2.2</i>	0.166	Supported
TIME	<---	COMMIT	<i>H2.3.2</i>	0.915	Supported
TIME	<---	ASSES	<i>H2.3.3</i>	-0.238	Not supported
TIME	<---	PROCED	<i>H2.3.4</i>	-0.434	Not supported
CUSTOMER	<---	PROCED		0.269	
TIME	<---	DOCUM	<i>H2.3.5</i>	0.516	Supported
TIME	<---	INCID	<i>H2.3.8</i>	-0.578	Not supported
CUSTOMER	<---	PARTNER	<i>H2.3.9</i>	0.220	Supported

Notes: Significant at $p < 0.05$.

The next step of the SEM analysis was conducted to test whether the relationships exist between the whole model and dependent variables, according to the main hypothesis *H2*. For this purpose, the independent variables were computed in SPSS, and the single independent variable of *EMSMM* was used to perform the next run of the SEM. To improve model fit characteristics a model re-specification was conducted (Recker, 2011). Specifically, some paths between independent and dependent variables were not significant. Besides, some relationships were observed between several dependent variables. Thus, the insignificant paths were deleted and some dependent variables, specifically SECURITY, SECRELAT and CUSTOMER, were used as mediators. As discussed earlier in this section, it is logical to assume that the category of *Security Related Performance* can be affected by the model through the category of *Security Performance*, as well as the category of *Market Performance* can be affected through *Customer Performance*. Besides, there was no significant direct relationship of the model on the category of *Time Performance* found. However, this category was impacted by the category of *Security Related Performance*. Indeed, *Vessels' schedule delays* and *Port State Control inspections* affect the total time vessel's operations.

After introduction of the discussed changes the SEM was run again. The model with the best model fit characteristics is shown in Figure 5.4. Its model fit characteristics, such as CMIN = 22.187; DF = 13; CMIN/DF = 1.707; CFI = 0.947; GFI = 0.945; AGFI = 0.881; NFI = 0.886; RMSEA = 0.083; PCLOSE = 0.168, contribute to the overall good fit of the structural model.

Figure 5.4 Results of the main SEM model with one independent and six dependent variables

Notes: Model fit statistics: CMIN = 22.187; DF = 13; CMIN/DF = 1.707; CFI = 0.947; GFI = 0.945; AGFI = 0.881; NFI = 0.886; RMSEA = 0.083; PCLOSE = 0.168; all coefficients are standardized; significant at $p < 0.05$.

Table 5.6 shows the results of hypothesis testing. It can be seen that the hypothesized relationship between EMSMM and SECURITY is significant ($\beta=0.415$), which supports *H2.1*. The positive link between EMSMM and RESILIENCE also exists, however it is not very strong ($\beta=0.074$), hence *H2.2* is supported. *H2.3* is supported partially, since the direct relationship exists only between EMSMM and CUSTOMER ($\beta=0.216$). However, other categories of *Other Organizational Performance*, namely, SECRELAT, MARKET and TIME, are positively impacted through mediators.

Table 5.6 Results of relationship testing between the EMSMM and organizational performance

Paths			Hypotheses	Standardized path coefficients	Results
SECURITY	<---	EMSMM	<i>H2.1</i>	0.415	Supported
RESILIENCE	<---	EMSMM	<i>H2.2</i>	0.074	Supported
CUSTOMER	<---	EMSMM	<i>H2.3</i>	0.216	Supported

Notes: Significant at $p < 0.05$.

The results of the data analysis, as shown in Figure 5.4 and Table 5.6, demonstrate a positive relationship of the model's implementation on business performance of the companies participating in the survey. That supports three sub-hypotheses of the second main hypothesis in this research. Specifically, the direct influence of the model on the security, business resilience and customer performance indicators can be observed. Besides, the measures of EMSMM have indirectly improved the security related, time and market performance indicators of the participating companies. Therefore, the results support the second main hypothesis of the thesis, which was formulated as follow:

“The EMSMM positively impacts organizational performance of shipping companies.”

5.4. Discussion

Firstly, in this chapter, the categories of organizational performance of shipping companies underwent tests by the EFA and CFA. The analyses resulted in six categories of organizational performance, namely, *Security Performance*, *Business Resilience*, *Market Performance*, *Time Performance*, *Security Related Performance*, and *Customer Performance*. The performance indicators associated with these categories are presented in Table 5.7. These indicators can be used by shipping and ship management companies to measure impacts of security management on different organizational performance, including not only security and resilience, but also other business performance. For this purpose, it is possible to use a method of measurement similar to the one used in this research. Specifically, it is recommended to compare performance in different years. Besides, as discussed in the literature review, it is also possible to compare organizational performance of the company with those of the competitors or industry average. However, it is important to note that this information might not be easily available because of the sensitivity of the topic.

The use of the suggested scale provides a link between security management and its impacts on organizational performance of the companies. This is one of the essential criteria for the effective security management. Being aware of areas of underperforming gives a possibility to focus on specific areas of security management. This was demonstrated through conducting the SEM.

Table 5.7 Categories of organizational performance of shipping companies and their indicators, as resulted from the analyses

Category	Performance Indicators
1. Security Performance	Number of cargo pilferage (cases)
	Number of stowaways (cases)
	Number of ship attacks, including terrorist and piracy attack, armed robbery (cases)
	Number of tampering with cargo, data and physical shipment (cases)
	Cargo loss and damage (dollars)
	Number of smuggling (cases)
	Number of violations of security rules by employees (cases)
2. Business Resilience	Time taken to identify security problems
	Time taken to mitigate security problems
	Time taken to recover from security incidents
3. Market Performance	Level of competitiveness
	Level of reputation for liability
4. Time Performance	Vessels' port turnaround time
	Vessels' total voyage time
5. Security Related Performance	Vessels' schedule delays because of security issues
	Number of Port State Control inspections on your company's vessels
	Additional cost because of security issues
6. Customer Performance	Level of flexibility in responding to customer requests
	Level of customers' overall satisfaction about physical resources
	Level of customers' overall satisfaction about quality of service provided
	Number of new customers
	Number of repeated customers

The relationship between the model's factors and each category of organizational performance were studied through the SEM analysis to test the second hypothesis in this study. As can be seen from Figure 5.3, the category of *Security Performance* is positively influenced by the factors of *Security Policy, System and Procedures* and *Business Partners Security*, whereas the category of *Security Performance* leads to a positive impact on *Security Related* and *Time Performance*. The respondents believed that well-structured security policies in the companies increase security awareness and therefore help to prevent security incidents or reduce the consequences. Also, in their opinion, "cooperation is

required for security management”. One of the respondents shared the opinion that “security is not something that can be only implemented by single party or single state, it can only be effective with the cooperation of all the parties”. This opinion supports the positive relationship between the factor of *Business Partners Security* and the category of *Security Performance*.

Besides, the category of *Customer Performance*, which is positively related to the category of *Market Performance*, is positively influenced by the factors of *Security Policy*, *System and Procedures* and *Business Partners Security*. This opinion was also shared by interviewees. Specifically, it was found during the interviews that implementation of procedures for controlling all documents, data and information, as well as procedures for reporting to relevant authorities of any incidents, help companies to keep customer information confidential and consequently improve customer satisfaction and the company’s image.

The category of *Business Resilience* is found to be positively influenced by the factor of *Management and Employee Commitment*. The respondents commented that it is generally difficult to measure resilience because of the low statistics of security incidents in the participating companies. One of the interviewees affirmed that according to his opinion “there’s no linkage between security management and business resilience”. That is a possible reason why the relationship between the EMSMM’s factors and this category is not very strong. However, they mentioned that based on the observations from training, drills and exercises for crisis management and continuity of operations, the employees became more knowledgeable and experienced in these areas:

The reaction to the accidents slightly improved since 2004. [To achieve these results] we have regular drills, trainings. The preparedness is always there!

Moreover, the factors of *Management and Employee Commitment* and *Documentation and Communication* showed positive relationships with 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 review of the literature presented in Section 2.4.1 showed

a negative impact on performance related to time. The interviewees often commented that for security management, “additional resources are required, including manpower, time, equipment and a lot of extra paperwork”. However, it is believed that the time performance should be improved when the effective security management becomes an integrated part of daily activities. One of the interviewees commented accordingly: “if you do it [security management] on every day basis, you can manage the time better”. Besides, it is worth mentioning that even though the negative relationships exist between some of the model’s factors and the category of *Time Performance*, it does not compromise the validity of the factors, since the whole model positively influences all categories of organizational performance (see Figure 5.4).

Besides, respondents also highlighted some other impacts of the implementation of the EMSMM on organizational performance. Firstly, clear identification of organizational roles and responsibilities, periodic self-assessment and training on crisis management resulted in positive changes of organizational procedures and technologies. Respondents believed that periodic assessment, as well as training, drills and exercises help their organizations to identify possible incident causes, whereas the identification of responsibilities helps to improve feedback and cooperation among employees. Additionally, one of them indicated that, after analysing the causes of security incidents, the organization usually introduced to their customers the new technologies or procedures, for example, GPS tracking or high security seals.

Secondly, the relationships between the EMSMM and the categories of organizational performance of shipping companies were analysed to test the second main hypothesis of the study. It can be seen from the Figure 5.4 that the model does have positive impacts on *Security Performance* and *Customer Performance*. This finding is supported by the following comment of one of the interviewees: “The general service we provide is better if the security management is better.” The category of *Security Performance* in its turn has positive relationship with *Security Related* and *Time Performance*, whereas the category of *Customer Performance* positively influences *Market Performance*. The following comment, made by one

of the interviewees, supports the positive relationship between the categories of *Customer Performance* and *Market Performance*:

The competitiveness can be lower because of the price, but branding is depending on what customers prefer. Our customers usually prefer better reputation and reliability to the price.

There is also a positive relationship existing between the model and the category of *Business Resilience*, however it is not significant, as explained earlier in this section.

Besides, it can be seen from Figures 5.3 and 5.4 that some categories of organizational performance are not directly affected by the model and its factors, but through other categories. For example, the category of *Security Performance* has a positive relationship with the category of *Security Related Performance* and subsequently on the category of *Time Performance*. Indeed, if security in a company is better, delays because of security issues and Port State Control inspections are less likely to happen, therefore the port turnaround time and voyage time are reduced. Similarly, the category of *Market Performance* is influenced by the model through the category of *Customer Performance*, which is understandable, since competitive position and reputation is generally connected to customer satisfaction and flexibility.

Additionally, the results of the SEM can be interpreted according to the ranking of the model's factors with regards to their importance for effective maritime security management provided in Section 4.7 of Chapter 4. As can be seen from Figure 5.3, the two most important factors COMMIT and PROCED have significant positive relationships with different categories of organizational performance, including SECURITY. Besides, the two least important factors DOCUM and PARTNER also showed significant positive impacts on organizational performance of shipping companies. It can be interpreted as follows: Even though these two factors are considered as the least important for the effective maritime security management by some of the participating companies, they have already shown some positive impacts on organizational performance of shipping companies, including *Security Performance*. Therefore, the managers of shipping companies

should not underestimate the importance of these factors when developing and implementing security management system in their companies.

Moreover, the third and the fourth most important factors (ASSES and COMMIT respectively) do not show any positive relationship with organizational performance, and only negatively influence TIME. As discussed earlier in this section, these negative impacts were expected. Besides, *Time Performance* can be improved when the EMSMM is implemented on a daily basis, since the overall impacts of the model are only positive, as Figure 5.4 shows. It might be concluded that to achieve positive impacts on the organizational performance of shipping companies, and subsequently a balance between security, resilience and other business performance, the EMSMM should be implemented integrally, specifically the factors of the EMSMM should be exercised together.

As discussed earlier, the proposed categorisation of the performance indicators of shipping companies (as shown in Table 5.7) can be used by managers for evaluation of the areas of security management that require improvements. The results of the conducted SEM analysis provide a basis for this evaluation. Thus, according to Figure 5.3 and Table 5.5, to improve *Security Performance* the management should mainly focus on measures associated with *Security Policy*, *System and Procedures* and *Business Partners Security*. These measures should also facilitate the improvement of *Security Related Performance*. The performance of *Business Resilience* can be strengthened through promoting *Management and Employee Commitment* to security management. When the company aims to improve *Customer and Market Performance* it is recommended in the first place to focus on activities associated with *Security Policy*, *System and Procedures* and *Business Partners Security*. When *Time Performance* requires improvements, it is necessary to ensure an implementation of the measures of *Management and Employee Commitment* and *Documentation and Communication*. Besides, it is important to conduct *Security Assessment* periodically, since it is an essential part of the effective maritime security management. Finally, the measures associated with *Security Incidents Handling and Continuity of Operations* should be always in place to ensure the required level of preparedness to security accidents.

5.5. Summary

In this chapter we aimed to examine the relationship between the proposed EMSMM for shipping companies and the organizational performance. The results presented in this chapter give answers to the third research question of this study. An analysis was conducted on the data collected from the survey with shipping and ship management companies all over the world. To prepare the foundation of the survey, the literature was examined on the questions of the effective security management in shipping companies and their organizational performance.

Firstly, through the literature review and further statistical analysis, the EMSMM, containing six factors, was developed, as shown in Chapter 4. Next, the three categories of organizational performance of shipping companies were also proposed, whereas some indicators were taken from the existing literature and some were suggested by the author. The proposed categorization had undergone a validity check by conducting pre-testing of the questionnaire. Further, statistical analyses, such as the EFA and the CFA, were conducted. As a result, one of the categories was divided into another four, which gives six categories of organizational performance of shipping companies, namely *Security Performance*, *Business Resilience*, *Market Performance*, *Time Performance*, *Security Related Performance*, and *Customer Performance*. The 22 performance indicators associated with these categories are shown in Table 5.7. Shipping and ship management companies are recommended using these indicators to measure their organizational performance with a purpose to understand how effective their security management is.

Secondly, through the SEM, the impacts of the model and its factors to categories of organizational performance of shipping companies were tested to answer the sub-research question 3.2 “*How do the EMSMM and its factors impact organizational performance of shipping companies?*”. The results indicated that the model and specifically the factors of *Security Policy, System and Procedures* and *Business Partners Security* positively impact the categories of *Security Performance* and *Customer Performance*. The category of *Security Performance* in its turn has positive impacts on *Security Related* and *Time Performance*, whereas the category of *Customer Performance* is positively related to *Market Performance*.

Besides, the factors of *Management and Employee Commitment* and *Documentation and Communication* positively influence the category of *Time Performance*, whereas the factors of *Security Policy, System and Procedures*, *Security Incidents Handling and Continuity of Operations*, and *Security Assessment* have a negative relationship with this category. The results of the statistical analysis were also supported by the findings from the exploratory interviews.

The tested relationships between the EMSMM's factors and the categories of organizational performance are important for the effective security management, because they link the management with its impacts. Based on this feedback managers can decide, which areas of security management require more attention when they aim to improve specific category of the company's performance.

CHAPTER 6. DISCUSSIONS AND CONCLUSIONS

6.1. Introduction

This is the final chapter of the thesis. It provides discussions and conclusions of this study on effective maritime security management in shipping companies. The chapter summarizes the findings and results according to the research questions presented in the introduction chapter. Managerial and academic implications of the results are presented next, followed by the research limitations. At the end of the chapter, future research directions are discussed.

6.2. Discussion of the Findings

This study closely follows scientific research process, which includes literature review, theory building and theory testing. First, as presented in Chapter 2, the literature review was conducted to prepare a theoretical background for the model building, as well as to answer several sub-research questions through analysis of the secondary data. Then, the EMSMM, including its nine factors, was developed in Chapter 3. For the purpose of this research, two main hypotheses were developed. To obtain preliminary information about the proposed model, thirteen in-depth structured interviews were conducted with industry practitioners. The main survey was administrated next, followed by the confirmatory survey. The hypothesis testing, including data analysis and results, is presented in Chapters 4 and 5. The methods of data analysis used in this research include thematic analysis and statistical methods, such as the EFA, the CFA, the SEM, and the AHP methodology. The results show that all two main hypotheses were partially supported. Table 6.1 presents the hypotheses and the outcomes.

Table 6.1 Hypothesis test summary table

Hypothesis		Outcome	
H1	The activities associated with the following nine groups are essential for the effective management of maritime security in shipping companies: <i>Security Culture; Management and Employee Commitment; Security Assessment; Security Policy, System and Procedures; Documentation and Communication; Process Control; Continuous Security Improvement; Security Incidents Handling and Continuity of Operations; and Business Partners Security.</i>	Partially supported	The activities associated with the following six groups are essential for the effective management of maritime security in shipping companies: <i>Management and Employee Commitment; Security Incidents Handling and Continuity of Operations; Security Policy, System and Procedures; Security Assessment; Documentation and Communication; and Business Partners Security.</i>
H2	The EMSMM positively impacts organizational performance of shipping companies.	Partially supported	The EMSMM positively influences the categories of <i>Security Performance, Business Resilience and Customer Performance</i> . Whereas <i>Security Performance</i> positively influences the category of <i>Security Related Performance</i> , which in turn has a positive impact on the category of <i>Time Performance</i> . Besides, <i>Customer Performance</i> has a positive relationship with the category of <i>Market Performance</i> .

The following section elaborates more on these results and discusses the findings according to the three main research questions of the thesis.

Research Question 1: What are the existing maritime security regulations and requirements for shipping companies?

The first aim of this thesis was *to study regulations and requirements on security management in shipping companies*. To achieve this aim, a secondary data

analysis through comprehensive literature review was conducted, followed by the exploratory interviews. The first research question was almost fully addressed in Chapter 2. The literature review on this question resulted in the list of maritime security regulations for shipping companies, presented in Table 2.1. This table and the discussion provide an answer to the sub-research question 2.1 regarding maritime security regulations. A deep analysis of these regulations resulted in a comprehensive list of compulsory and voluntary maritime security requirements, presented in Table 2.2. After a discussion on the existing situation with implementation of the requirements, Table 2.2 was further developed to Table 2.3, where the summarized list of the requirements is provided. The list of the requirements contributes to the sub-research question 2.2 of this study.

The literature review showed that the implementation of these requirements in the area was not investigated much. Thus, to fill this gap and to answer the sub-research question 1.3, the exploratory interviews were conducted to study how maritime security requirements are implemented in shipping companies. The results showed that the interviewed companies have implemented a majority of the listed compulsory requirements. However, as some interviewees mentioned, the main reason for the implementation was their mandatory nature. The level of implementation of the voluntary requirements varies significantly. Some interviewees mentioned that the implementation of the voluntary requirements increases their security level significantly. Some companies even implemented other security measures, besides those from the list. Meanwhile, other interviewees shared the opinion that these requirements were implemented mostly to comply with the needs of their customers and partners. Additionally, some respondents believed that the compliance with the voluntary programmes has become a prerequisite to participate in the international trade. Generally, the interviewees agreed that the implementation of requirements and their effectiveness significantly depends on the management approach chosen by a company.

Research Question 2: How can maritime security be managed effectively in shipping companies?

To achieve the second aim of this thesis, which is *to develop and validate the effective maritime security management model (EMSMM) for shipping companies*,

the second research question has been answered. Firstly, the sub-research question 2.1 regarding the applicable approaches to the security management in shipping companies and existing management frameworks was addressed. Findings of the secondary data analysis conducted through the literature review on this topic showed that there are several management approaches, which are applicable for the management of maritime security, namely, risk management (RM), quality management (QM) or total quality management (TQM), business continuity management (BCM), disaster management (DM), crisis management (CM) and security management (SM) or total security management (TSM). The publications where these approaches were applied for maritime security management were summarized in Table 2.4. Additionally, Chapter 2 provides a review of frameworks and models proposed by researchers with the purpose of security management in shipping and supply chain companies. However, it was observed that there are a number of problems which shipping companies experienced when managing maritime security. The problems include overlapping and inconsistency between the requirements imposed by different regulatory documents, the need for unification of the existing common standards and maritime regulations, the need for a comprehensive security management framework, as well as specific and detailed guidelines for security management. Besides, the difficulties in measuring and understanding the impacts of the implementation of security requirements on organizational performance significantly affect the implementation of these requirements in shipping companies. These results contribute to the sub-research question 2.2 regarding the existing problems in management of maritime security in shipping companies.

The lessons from the existing frameworks and models for security management as well as the discussed problems were analysed and a list of essential criteria for the EMSMM was proposed to answer the sub-research question 2.3 of this research. The list includes the following seven criteria:

1. *The EMSMM is easily applicable in practice and provides guidance for implementation.*
2. *The EMSMM helps managers to implement compulsory and voluntary maritime security requirements.*

3. *The EMSMM is developed specifically for shipping companies.*
4. *The EMSMM aims to achieve the balance between security, efficiency and resilience.*
5. *The EMSMM links security management and its impacts on organizational performance.*
6. *The EMSMM is based on the holistic approach to security management.*
7. *Finally, the EMSMM is easily adopted by different shipping organizations.*

The result of analysis of the existing frameworks and models based on the proposed criteria is shown in Table 2.5.

The sub-research question 2.4 is about the model and its factors. This research question was addressed in Chapters 3 and 4 of the thesis. The EMSMM's development was presented in Chapter 3 of this thesis. The factors of the model were derived based on the management approaches and with the consideration of earlier proposed frameworks and models for security management in shipping and supply chain companies. The proposed model satisfies the seven essential criteria, as shown in Table 3.2. The EMSMM was further validated by conducting exploratory interviews and the main survey. The analysis of the collected data through the EFA and CFA resulted in the EMSMM, containing six factors and 22 associated attributes. The factors of the model include *Management and Employee Commitment*, *Security Assessment*, *Security Policy*, *System and Procedures*, *Documentation and Communication*, *Security Incidents Handling and Continuity of Operations*, and *Business Partners Security*.

Then the importance of these factors was ranked based on the results of the AHP survey. The results are presented in Figure 4.11. They show that a lot of attention is currently given to the areas of management, which focus on reducing human errors, specifically to the factors of *Management and Employee Commitment*, *Security Incidents Handling and Continuity of Operations* and *Security Policy*, *System and Procedures*. These factors were ranked as the three most important factors of the model, following by the factors of *Security Assessment* and *Documentation and Communication*. The factor of *Business Partners Security* was rated as the least important factor. However, it was observed based on the results of the interviews that this factor is becoming more and more

important for security improvement. Indeed, the culture of maintaining security between business partners can help not only to increase security within the company and its direct partners, but also to strengthen the whole supply chain security.

Generally, the results showed that all six factors of the EMSMM were considered as very important areas of management for security improvement. Therefore, it is essential for shipping companies to implement the attributes associated with these factors simultaneously. The prioritisation of the chosen measures can be made based on the results provided in Table 4.11. Besides, more attention can be given to some of the factors according to the impacts of security management on business performance of the companies. To provide more explanation, the third research question of the study was addressed.

Research Question 3: What are the impacts of maritime security management on organizational performance of shipping companies?

The third research aim of this study is *to understand the impacts of maritime security management on organizational performance of shipping companies*. To answer the sub-research question 3.1 “*What are the reported and proposed impacts of the implementation of maritime security initiatives on organizational performance of shipping companies?*”, a secondary data analysis through a comprehensive review of the literature on this topic was conducted first. The analysis of the impacts, discussed in different sources, resulted in Table 2.8, which summarized the impacts based on several criteria, such as positive and negative, reported and proposed, and short-term and long-term impacts. It can be seen from the table, that some companies have experienced unexpected negative impacts and some did not achieved a number of proposed benefits. However, positive impacts were also reported. It leads to the conclusion that the impacts vary in different companies and significantly depend on security management approach.

To provide a background for the collection and analysis of the primary data, the literature on organizational performance of shipping companies was reviewed and resulted in the following conclusions:

- There are four most common categories of organizational performance found in the literature: *financial*, *market*, *internal business* and *customer performance* (Table 2.10).
- In a majority of studies on the impacts of security on organizational performance of shipping and supply chain companies, mostly the indicators from the categories of *internal business* and *customer performance* were used. Besides, these security indicators are not detailed enough to measure security improvement precisely.
- There are few studies found where security and resilience indicators are detailed and presented in separate categories. However, the lists of other organizational performance used in this studies are not comprehensive and do not include a number of indicators, listed in Table 2.10.

Thus, to address the existing gaps in the literature on the impacts of security management on organizational performance, and since one of the main objectives of the proposed EMSMM is to achieve the balance between security, resilience and efficiency, the three categories of organizational performance of shipping companies were developed in Chapter 3 and validated in Chapter 5.

Through the process of validation, one of the categories was divided into four, which resulted in six categories of organizational performance, namely, *Security Performance*, *Business Resilience*, *Market Performance*, *Time Performance*, *Security Related Performance*, and *Customer Performance*.

Finally, the testing of relationships between the EMSMM and organizational performance through the SEM was conducted in Chapter 5. The results contribute to the sub-research question 3.2 of this study “*How do the EMSMM and its factors impact organizational performance of shipping companies?*” It was observed that the model and specifically the factors of *Security Policy, System and Procedures* and *Business Partners Security* have positive relationships with the categories of *Security Performance* and *Customer Performance*. The category of *Security Performance* in its turn positively influences *Security Related* and *Time Performance*, whereas the category of *Customer Performance* has a positive relationship with *Market Performance*. Additionally, the category of *Time Performance* is positively affected by the factors of *Management and Employee*

Commitment and *Documentation and Communication* and negatively affected by the factors of *Security Policy, System and Procedures*, *Security Incidents Handling and Continuity of Operations*, and *Security Assessment*. The relationship between the model and the category of *Business Resilience* was not significant, which can be explained by a low number of records on security accidents which threaten business resilience in the companies participating in the survey. It might be concluded that the implementation of the proposed EMSMM leads to visible improvements not only of the security performance, but also of other business performance of shipping companies. The implications of the proposed model are discussed in detail in the following section.

6.3. Implications

This research aims to answer three primary research questions on the topic of effective maritime security management in shipping companies. The study has many contributions to academia as well as management and regulatory practice. The contributions are discussed below according to the research questions.

6.3.1. Academic Implications

Firstly, this study contributes significantly by providing a comprehensive review of maritime security regulations and requirements for shipping companies. This work analyses compulsory and voluntary requirements and summarises them into categories as well as investigates the problems related to their implementation. It was concluded from the literature review that the implementation and effectiveness of both compulsory and voluntary security requirements have not been studied intensively. Thus, to address the existing gaps, the factual implementation of the requirements was investigated to understand what security measures are implemented in shipping companies and effective for security improvement. The results of this investigation should be used by researchers in the field of effective management of security in shipping and supply chain companies, because it provides an understanding of companies' attitude towards complying

with mandatory and voluntary regulations. Besides, the analysis and classification of the regulations and requirements for shipping companies, provided in this thesis, can be further used by researchers and analysts in different areas, such as business studies, studies on law and regulations, engineering and technical science, etc.

Secondly, this research thesis contributes to fill gaps in the literature on maritime security management in shipping companies by providing a comprehensive review of existing approaches to security management. It also examines management models and frameworks developed earlier by other researchers and industry practitioners to show their strengths and weaknesses. Besides, the literature review on this topic includes a discussion on the main problems that shipping companies generally face when managing security. This comprehensive literature review resulted in the list of seven essential criteria for the EMSMM. The developed criteria should be reformulated and used for security management model in other companies of the supply chain, besides they can be used for other areas of management in shipping and supply chain companies.

One of the important contributions of this study to the research on the topic of maritime security management is the introduction of the EMSMM for shipping companies. The model's factors were developed based on the lessons learnt from other academic and industrial publications. The proposed EMSMM improves the existing models by focusing on the uncovered problems. Specifically, it stimulates the implementation of existing security requirements and helps to balance security, efficiency and resilience. The industry practitioners' opinion about the model and its factors was investigated by conducting the two surveys with target population consisting of shipping and ship management companies all over the world. The model was validated through thematic, statistical and AHP analyses. The validated EMSMM is therefore a contribution to the research of security management in shipping companies because it combines the important security management aspects that shipping companies should focus on. Besides, this study is one of the first studies, using the AHP methodology to rank the importance of the model's factors for security improvement.

Thirdly, this research provides a significant contribution to the literature on the impacts of maritime security management on organizational performance. It not

only combines some empirical evidence available from various sources, but also summarizes the impacts according to different classifications used by other researchers. Firstly, the lists of reviewed positive and negative impacts were composed. Further, two other levels of classification were added, namely, proposed and reported, and short-term and long-term impacts. It is important to apply all levels of classification simultaneously when reviewing the impacts, because the addition of every level adds some new important information. Hence, the categorization of the impacts proposed in this research should be further used by other researchers in this and relevant areas, and the list of impacts, combined in the Chapter 2 of the thesis, should be used in future studies by being supplemented with new available data.

Moreover, for the question of the impacts of maritime security management on organizational performance of shipping companies, the literature on categories and indicators of organizational performance was reviewed. The review resulted in the scale containing six categories of performance, which were validated and used in this research to collect the information on how the EMSMM impacts organizational performance of the companies participating in the survey. It is highly recommended for other researchers to use the scale for collection of the information about the link between security management and performance of shipping and supply chain companies. Besides, to choose the method of measurement the author has conducted a comprehensive review of the relating literature. Various possibilities to measure the impacts of security management on performance indicators were considered and discussed. This discussion contributes to the research on the topic of business performance measurement by explaining the possibilities to use the proposed scale in a combination with other measurement methods, and their strengths and weaknesses.

Besides, the thesis represents one of the first studies conducted on the impacts of effective security management in shipping companies on their organizational performance. It does not only show the effectiveness of the proposed model, but also describes the relationship between its factors and categories of organizational performance. The links between maritime security management and organizational

performance of shipping companies have not been investigated in detail before, thus the study can be considered as a pioneering research on this topic.

6.3.2. Managerial and Regulatory Implications

In addition to having a strong theoretical contribution to academia and future research, this thesis provides some managerial and legal insights. As one of the outputs of this research, an Executive Summary of the results is composed and distributed among the participants of the interviews and surveys. The summary provides short information about the research background, problems, aims and methodology. It also presents the results of this study in a way to show usefulness and practical implications to practitioners of the shipping industry. This section presents a discussion on the managerial implications of the results of this study and implications for policy makers.

Firstly, Chapter 2 offers comprehensive lists of maritime security regulations and requirements which can give shipping companies some background information about the maritime security regime. The composed tables on regulations and requirements show the conditions for compliance with some regulations and for implementation of specific requirements (for example, trading area of the company; or compulsory / voluntary character of the requirements). Additionally, they present similarities and differences between various regulations and requirements. Besides, the discussion on the implementation and effectiveness of different security measures, as well as on the problems associated with maritime security management, might be in the interests of industry practitioners, since it shows different approaches to implementation of these measures and experience in security management in different companies. From this, managers can see that the same security measure might be more effective or less effective depending on the management approach chosen by their companies.

One of the most significant managerial implications of this research is the proposed EMSMM. The model was developed specifically for shipping companies with the consideration of their features and is expected to help them to achieve a balance between security performance, business resilience and other organizational

performance. It can be used as a toolkit or guidance for security managers in shipping companies in evaluating their security management policies and strategies. Along the line, this will facilitate the benchmarking of security management among shipping companies and contribute to the standardisation of the industry's security management practices. Thus, policy makers should use the proposed model for further redevelopment and improvement of the existing guidance and best practice recommendations. The proposed scale for performance measurement should be included in the guidance. The discussed improvements are expected to facilitate implementation of the compulsory and voluntary requirements. Besides, the study provides a ranking of the model's factors according to their importance for the effective security management. The results indicate areas of security management requiring more attention. This ranking is expected to help managers in decision-making regarding investments in security measures, personnel allocation and general planning of security related activities.

Next, the study offers detailed information about the impacts of maritime security management on organizational performance of shipping companies. Managers should know the changes experienced by other companies. It is important for them to see all positive and negative impacts of security management to understand the importance of its implementation and to adapt their management approach to avoid or reduce negative impacts. It is worth mentioning that the negative relationship between some of the model's factors and one of the categories of organizational performance does not compromise the validity of the model and its factors, since the whole model was found to be positively influencing all categories of organizational performance. Thus, to achieve the expected benefits, all factors should be implemented together.

Additionally, the thesis presents the categories and indicators of organizational performance, which will likely be used by shipping companies to measure performance changes caused by security management. There are a number of different methods to use the proposed scale for performance measurement. For instance, besides the way used by the author (comparison of performance in different years), it is also possible to compare the company's performance with the industry average or with performance of the company's main competitor. However,

the last two methods might be problematic because of the sensitivity of the required information.

After assessment of the organizational performance is conducted using the proposed scale, the next step should be implementation of the necessary actions. The results of this research show positive and negative relationships between factors of the EMSMM and categories of organizational performance. The knowledge about the relationships should be used to adjust security management strategy in shipping companies according to observed changes in their performance. Based on the assessment managers can decide, which areas of security management require more attention when they aim to improve specific category of the company's performance. The discussed managerial implications were summarised into a set of recommendations to shipping and ship management companies on effective management of maritime security.

6.3.2.1. Recommendations to Shipping and Ship Management Companies on Effective Management of Maritime Security

Management of maritime security might be a complex process. Choosing a wrong approach to security management and underestimating its importance might lead to negative results, such as low security level in the company and its vessels, high number of security accidents and violations and consequently often Port State Control inspections and detentions. This might not only negatively affect the company's financial statements, but also harm its reputation. However, it is possible to manage maritime security effectively and to achieve a balance between security, resilience and effectiveness. Therefore, the effective security management not only results in improvements in security performance of the company, but it also positively impacts other organizational performance, such as business resilience, market and customer performance, time performance and other security related performance. To achieve the discussed results, it is strongly recommended to focus on the following six areas of security management and their associated attributes:

1. Management and Employee Commitment to Security

- Security related roles and responsibilities are clearly identified and documented for employees;
- Procedures for employees to report security errors and breaches are established;

2. Security Incidents Handling and Continuity of Operations

- Disaster, crisis management and emergency plans are developed based on considered scenarios;
- Training and drills on disaster and crisis management are periodically conducted;
- Dedicated communication channels exist for emergency cases;

3. Security Policy, System and Procedures

- A well-structured security management policy is developed and documented;
- Security management policy includes security management system, procedures, plans, etc;
- Security policy is included in overall company policy;
- Security policy, system, procedures, plans do not contradict with other measures and procedures;
- Security measures are integrated into daily activities;

4. Security Assessment

Security risk assessment is conducted to derive a risk magnitude.

Risk acceptance levels are established based on risk magnitudes and existing control barriers.

Measures are implemented to mitigate identified risks according to risk acceptance levels.

5. Documentation and Communication Security

- Measures to secure organizational documentation and information are developed and implemented;
- Data and processes in the communication system are periodically backed up;
- Documentation and information systems are periodically backed up;
- IT security measures are implemented;

6. Business Partners Security

- Collaboration with business partners exists to identify, mitigate and share security risks;
- Liabilities for possible security incidents are clearly defined in contracts with business partners;
- Security trainings and exercises are jointly organized with business partners;
- All current partners are periodically assessed to ensure their compliance with security requirements;
- All future business partners undergo security background checks.

Next, to understand the impacts of security management on the company's performance and therefore its effectiveness, it is recommended to conduct periodical assessment of the organizational performance, specifically security performance, business resilience and other business performance of the company. For this purpose companies are recommended to use the following scale of organizational performance indicators to measure impacts of security management:

1. Security Performance

- Number of cargo pilferage (cases);
- Number of stowaways (cases);
- Number of ship attacks, including terrorist and piracy attack, armed robbery (cases);
- Number of tampering with cargo, data and physical shipment (cases);
- Cargo loss and damage (dollars);
- Number of smuggling (cases);
- Number of violations of security rules by employees (cases);

2. Business Resilience

- Time taken to identify security problems;
- Time taken to mitigate security problems;
- Time taken to recover from security incidents;

3. Market Performance

Level of competitiveness

Level of reputation for liability

4. Time Performance

- Vessels' port turnaround time;
- Vessels' total voyage time;

5. Security Related Performance

- Vessels' schedule delays because of security issues;
- Number of Port State Control inspections on your company's vessels;
- Additional cost because of security issues;

6. Customer Performance

- Level of flexibility in responding to customer requests;
- Level of customers' overall satisfaction about physical resources;
- Level of customers' overall satisfaction about quality of service provided;
- Number of new customers;
- Number of repeated customers.

To measure the performance, it is recommended to use the comparison in different years. Besides, it is also possible to compare the company's performance with those of the main competitors or leaders in the industry. The difficulties however might be caused by sensitivity of the topic and lack of the required information.

After the performance assessment is conducted, the next step is to introduce necessary changes in the security management based on the assessment's results. First, it is necessary to understand, in which categories of the organizational performance the company underperforms. Then, necessary changes might be introduced based on the following relationships:

- To improve *Security Performance* the management should mainly focus on measures associated with *Security Policy, System and Procedures (3)* and *Business Partners Security (6)*. These measures should also facilitate the improvement of *Security Related Performance*.

- The performance of *Business Resilience* can be strengthened through promoting *Management and Employee Commitment to security (1)*.

- When the company aims to improve *Customer and Market Performance* it is recommended in the first place to focus on activities associated with *Security Policy, System and Procedures (3)* and *Business Partners Security (6)*.

- When *Time Performance* requires improvements, it is necessary to ensure an implementation of the measures of *Management and Employee Commitment (1)* and *Documentation and Communication Security (5)*.

- It is important to conduct *Security Assessment (4)* periodically, since it is an essential part of the effective maritime security management.

- The measures associated with *Security Incidents Handling and Continuity of Operations (2)* should be always in place to ensure the required level of preparedness to security accidents.

To introduce the necessary measures it is recommended to focus on the associated activities, as discussed earlier. However, it is highly important to implement actions according to the company's features and existing management activities. Therefore, it is strongly recommended to adapt the proposed guidance to the overall management of the company.

6.4. Research Limitations

Several limitations of this research should be mentioned. Firstly, some limitations might be related to the development of the measurement items. As mentioned earlier, the proposed model was partly developed with consideration of other similar constructs, and some factors and attributes were proposed in this study. This limitation was mitigated by a face validity check of both parts, the model and the organizational performance scale, convergent and discriminant validity check and further validation through statistical analyses. However, it is believed that subjective bias still exists.

Secondly, the performance measurement indicators used in this research might add some limitations. As discussed in Chapter 2, using objective measures would be ideal to collect the information regarding changes in organizational performance. However, it was not possible to obtain information about real performance in this

research. Thus, to improve the reliability of the collected information, a combination of subjective and quasi-objective measures was used.

Another limitation might be related to the respondents' awareness of organizational performance asked in the survey. Since the target population in this research consists of managers who are in charge of security in shipping companies, it is difficult to know exactly if the respondents keep track of other organizational performance of their companies. During the survey, participants were recommended to involve their colleagues if they have doubt regarding some questions on organizational performance. However, the author cannot guarantee that the respondents followed the suggestion. Thus, it is possible that some questions regarding performance indicators were not answered with full knowledge.

The fourth limitation of this research involves a tendency of shipping companies to underestimate security incidents and overestimate security and other related improvements due to fear of reputation loss, lower competitiveness, increase of insurance premiums and other possible consequences. In this study, the questionnaire was carefully designed to reduce this limitation as much as possible.

The lower response rate of 3.5% is considered the fifth limitation in this study. However, as discussed earlier, the low response rate was expected due to a number of reasons, particularly, the sensitivity of the topic, length of the questionnaire, difficulties to target directly the correct person (responsible for security management) in a company, and other factors. To increase the response rate, several follow-up emails were sent after the main mail-out. Multiple mail-outs might cause a non-response bias. However, the results of ANOVA test indicated that non-response bias was not an issue in this research.

Sixth, the systematic error introduced by a single source of data collection might be one of the limitations in this research. When independent and dependent variables are collected in a single survey, it might lead to a common method bias. Many possible ways to avoid a common method bias were suggested by researchers. For the purpose of this study, the approach introduced by Podsakoff et al. (2003) was applied. To retrieve the common variance, a common latent factor was introduced and retained in the measurement model for a further statistical analysis. Besides, several limitations of the methods of data collection and analysis,

including the AHP methodology, as well as possible ways to address them, were discussed in Chapters 3 and 4.

Finally, another limitation is related to the lack of collected data on security accidents which threaten business resilience. As can be seen from the results of the SEM, the relationship between the introduced model and the category of *Business Resilience* is not significant. Since a majority of the responding companies did not experience real cases where business resilience was threatened, they were only able to indicate the changes of this performance based on the trainings and exercises. To address this limitation, further research is needed. The next section discusses possible directions for future research.

6.5. Future Research

Several ideas for a future research on the studied area can be drawn from the results of this study. First, the presented list of impacts of maritime security management on organizational performance should be further elaborated by adding more available information. Ideally, the information on the impacts should be collected together with information on security management in a company. This may help to create a clearer understanding of the links between security management and performance of shipping companies.

Additionally, there are some improvements which might be done on the performance measurement scale used in this research. The development of the scale can be conducted in two ways. For scientific purposes, the scale can be amended to ensure more use of available objective information in combination with subjective and quasi-objective measures. The collection of this comprehensive information is a lengthy and time-consuming process requiring the use of various sources, which are sometimes not available to the public, and can be developed as an independent research project. Besides, the proposed measurement scale might be in the interests of industry participants. Specifically, shipping companies are advised to use it for measuring the effectiveness of the implemented security management practice. For that purpose, the performance indicators should be amended to ensure reliable information which can be collected from various sources inside and outside the

company, including technical management department, financial department, direct partners and customers, and other sources. The overall information collected by using the suggested method can give a precise picture on the links between security management and organizational performance.

Another possible area for future research is to study more in details the implementation of the proposed EMSMM in shipping companies. One of the methods to examine how the model is implemented in shipping companies and how it impacts organizational performance is to conduct a case study research. This method also allows investigating more on possible follow-up actions to improve security management according to reported changes in organizational performance.

Besides, to mitigate the limitations discussed in the previous section, further research is recommended to find out if there is a positive relationship between the EMSMM and *Business Resilience* performance. For this purpose, the sample population should be constructed from companies with records of security accidents which threaten their business resilience.

Finally, one of the possible directions for a further improvement is a collaborative work with IT developers, which should result in an interactive assessment tool for shipping and ship management companies. After entering a required data on specific performance indicators, the user receives an assessment report, which shows how performance of the company has been changed. Alternatively, the performance can be shown in a comparison with industry average or best practice organizations. Apart from the performance assessment, the report indicates areas of security management that require special attention and includes recommendations or strategies for further improvements. This assessment tool might be also interesting for companies, providing external management and consulting with a focus on security management.

REFERENCES

- Acciaro, M. and Serra, P. (2013) "Maritime Supply Chain Security: A Critical Review", Paper presented at the International Forum on Shipping Ports and Airports (IFSPA), 3-5 June, Hong Kong.
- APEC (2002) Secure Trade in the APEC Region (STAR) Initiative, APEC private sector, Supply chain security guidelines, Asia-Pacific Economic Cooperation.
- Arunraj, N. S. and Maiti, J. (2010) "Risk-based maintenance policy selection using AHP and goal programming", Safety Science, Vol. 48, No. 2, pp. 238–247.
- Autry, C. W. and Bobbitt, L. M. (2008) "Supply chain security orientation: conceptual development and a proposed framework", International Journal of Logistics Management, Vol. 19, No. 1, pp. 42-64.
- Barzilai, J. (2005) "Measurement and preference function modelling", International Transactions in Operational Research, Vol. 12, No. 2, pp. 173–183.
- Banomyong, R. (2005) "The impact of port and trade security initiatives on maritime supply-chain management", Maritime Policy and Management, Vol. 32, No. 1, pp. 3-13.
- Barnes, P. and Oloruntoba, R. (2005) "Assurance of security in maritime supply chains: Conceptual issues of vulnerability and crisis management", Journal of International Management, Vol. 11, No. 4, pp. 519-540.
- BASC (2002) BASC Standards, Business Alliance for Secure Commerce.
- Bernard, R. (2009) "Securing the Supply Chain", Security Technology Executive Magazine, July 2009, pp. 20-23.
- Bhatnagar, R. and Sohal, A. S. (2005) "Supply chain competitiveness: measuring the impact of location factors, uncertainty and manufacturing practices", Technovation, Vol. 25, No. 5, pp. 443-456.

Bichou, K. (2004) “The ISPS Code and The Cost of Port Compliance: An Initial Logistics and Supply Chain Framework for Port Security Assessment and Management”, Maritime Economics and Logistics, Vol. 6, No. 4, pp. 322-348.

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. (2011) “Assessing the impact of procedural security on container port efficiency”, Maritime Economics and Logistics, Vol. 13, No. 1, pp. 1-28.

Bichou, K. and Gray, R. (2004) “A logistics and supply chain management approach to port performance measurement”, Maritime Policy and Management, Vol. 31, No. 1, pp. 47-67.

Bichou, K., Lai, K. H., Lun, Y. H. V. and Cheng, T. C. E. (2007) “A quality management framework for liner shipping companies to implement the 24-Hour Advance Vessel Manifest Rule”, Transportation Journal, Vol. 46, No. 1, pp. 5-21.

Bichou, K., Szyliowicz, 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.

Bollen, K. A. (1989) Structural Equations with Latent Variables, Wiley, New York.

Borger J. and Whitaker B. (2003) “US watching al-Qaida’s fleet”, The (London) Guardian, January 1, 2003,
<http://www.guardian.co.uk/international/story/0,3604,867160,00.html>, accessed 21 February 2015.

Boyne, G. A., Meier, K. J., O’Toole, L. J. Jr. and Walker, R. M. (2006) Public service performance: perspectives on measurement and management, Cambridge University Press, Cambridge.

Brewer, P. C. and Speh, T. W. (2000) "Using the balanced scorecard to measure supply chain performance", Journal of Business Logistics, Vol. 21 No. 1, pp. 75-93.

Bryant, D. L. (2009) "The outlook for maritime security", Journal of Commerce, 12 January, p. 56.

Burns, M. G. (2013) "Estimating the impact of maritime security: financial tradeoffs between security and efficiency", Journal of Transportation Security, Vol. 6, No 4., pp. 329-338.

Byun, D. H. (2001) "The AHP approach for selecting an automobile purchase model", Information and Management, Vol. 38, pp. 289-297.

CBP (2001) Customs-Trade Partnership Against Terrorism, Customs and Border Protection, U.S.

CBP (2002) Container Security Initiative, Customs and Border Protection, U.S.

CBP (2009) Import Security Filing and Additional Requirements, 10 plus 2 Rule, Customs and Border Protection, U.S.

CBSA (1994) Partners in protection (PIP), Canada Border Service Agency, Canada.

CBSA (2004) 24 Hour Advance Manifest Rule, Canada Border Services Agency, Canada.

Chan, A. H., Kwok, W. Y. and Duffy, V. G. (2004) "Using AHP for determining priority in a safety management system", Industrial Management and Data Systems, Vol. 104, No. 5, pp. 430-445.

Charnes, A., Cooper, W. W. and Rhodes, E. (1978) "Measuring the efficiency of decision making units", European Journal of Operational Research, Vol. 2, pp. 429-444.

Chen, Y. H., Chen, S. L. and Wu, C. H. (2005) "The Impact of Stowaways and Illegal Migrants by Sea - a case study in Taiwan", Paper presented at the International Association of Maritime Universities (IAMU) 6th Annual General

Assembly and Conference, 24-26 October, Malmo, Sweden.

China Custom (2008) Measures for Manifest Administration For Inbound and Outbound Means of Transportation of The People's Republic of China, The People's Republic of China.

Choe, K., Booth, D. and Hu, M. (1997) "Production competence and its impact on business performance", Journal of Manufacturing Systems, Vol.16 No. 6, pp. 409-421.

Christopher, K. (2009) Port Security Management, Taylor and Francis Group, London.

Churchill, G. A. (1991) Marketing Research: Methodological Foundations, The Dryden Press, London.

Cleveland, G., Schroeder, R. G. and Anderson, J. C. (1989) "A Theory Of Production Competence", Decision Sciences, Vol. 20 No. 4, pp. 655-668.

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.

Closs, D. J., and McGarrell, E. F. (2004) "Enhancing Security Throughout the Supply Chain", IBM Center for the Business of Government, U.S.

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.

Customs Service (2003) Secure Exports Partnership, Important Information for applicants, Customs Service, New Zealand.

Dagkinis, I. and Nikitakos, N. (2013) "Enhance of ship safety based on maintenance strategies by applying of Analytic Hierarchy Process", SPOUDAI - Journal of Economics and Business, Vol. 63, No. 3/4,

<http://spoudai.unipi.gr/index.php/spoudai/article/view/86/131>, accessed on 12 June 2014.

Dawes, J. (1999) “The Relationship between Subjective and Objective Company Performance Measures in Market Orientation Research: Further Empirical Evidence”, Marketing Bulletin, Vol. 10, No. 3, pp. 65-75.

Dawson, C. (2002) Practical Research Methods, UBS Publishers’ Distributors, New Delhi.

Dess, G. G. and Robinson, R. B. Jr. (1984) “Measuring Organizational Performance in the Absence of Objective Measures: The Case of the Privately-Held Firm and Conglomerate Business Unit”, Strategic Management Journal, Vol. 5, No. 3, pp. 265-273.

DHS (2003) Code of Federal Regulations Title 33: Navigation and Navigable Waters. Subpart C – Notification of Arrival, Hazardous Conditions, and Certain Dangerous Cargos, Department of Homeland Security, U.S.

Dillman D. (2001) Mail and Internet Surveys: The Tailored Design Method, John Wiley, New York.

Donegan, H., Dodd, F. and Mc Master, T. B. M. (1992) “A New Approach to the AHP Decision Making”, The Statistician, Vol. 41, No. 3, pp. 291-305.

DoT (2002) Presentation of Vessel Cargo Declaration to Customs Before Cargo Is Laden Aboard Vessel at Foreign Port for Transport to the United States, 24 Hours Rule, Department of Treasury, U.S.

DoT (2005) The National Strategy for Maritime Security, Department of Treasury, U.S.

EU (1994) Community Customs Code, European Union.

EU (2004) Regulation on enhancing ship and port facility security, European Union.

EU (2007) Authorized Economic Operators Programme, European Union.

EU (2011) EU Advance Cargo Security Rules, EU 24 hour rule, European Union.

Evans, J. R. (2007) “Impacts of information management on business performance”, Benchmarking: An International Journal, Vol. 14, No. 4, pp. 517-533.

Eyefortransport (2002) Cargo security overview: Technologies, Government and Customs Initiatives, <http://www.solomonchen.name/download/7ms/1-034-cargosecurity.pdf>, accessed 24 June 2014.

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.

Field, A. (2000) Discovering Statistics using SPSS for Windows, Sage publications, London – Thousand Oaks – New Delhi.

Fletcher, T. (2007) “Authorized Economic Operator (AEO) Programs: IBM’s perspective”, World Customs Journal, Vol. 1, No. 2, pp. 61-65.

Fornell, C. and Larcker, F. (1981) “Evaluating Structural Equation Models with Unobservable Variables and Measurement Error”, Journal of Marketing Research, Vol. 18, No. 1, pp. 39-50.

Frankel, E. G. (1993) “Total quality management in liner shipping”, Marine Policy, Vol. 17, No. 1, pp. 58-63.

Fu X., Ng A. K. Y. and Lau Y. Y. (2010) “The impacts of maritime piracy on global economic development: the case of Somalia”, Maritime Policy and Management, Vol. 37, No. 7, pp. 677-697.

Gay, L. R. and Airasian, P. (2003) Educational Research: Competencies for Analysis and Applications, 7th ed., Pearson Education, Upper Saddle River, NJ.

González-Benito, J. (2007) “A theory of purchasing’s contribution to business performance”, Journal of Operations Management, Vol. 25, No. 4, pp. 901-917.

González-Benito, Ó. and González-Benito, J. (2005) “Cultural vs. operational market orientation and objective vs. subjective performance: Perspective of production and operations”, Industrial Marketing Management, Vol. 34, No. 8, pp. 797-829.

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, <http://spoudai.unipi.gr/index.php/spoudai/article/view/52>, accessed 2 July 2014.

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.

Gujar, G., Yan, H. and Nankivell, K. L. (2013) “A Systemic View of Container Security: A Need for Strategic Cooperative Management”, Paper presented at the International Forum on Shipping Ports and Airports (IFSPA), 3-5 June, Hong Kong.

Gunasekaran, A., Patel, C. and McGaughey, R. E. (2004) “A framework for supply chain performance measurement”, International Journal of Production Economics, Vol. 87, No. 3, pp. 333-347.

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

Gutierrez, X. and Hintsa, J. (2006) “Voluntary supply chain security programs: a systematic comparison”, Paper presented at the International Conference on

Information Systems, Logistics and Supply Chain (ILS'06), 15-17 May, Lyon, France.

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. F., Anderson, R. F., Tatham, R. L. and Black, W. C. (1995) Multivariate Data Analysis with Readings, Pearson Prentice Hall, Upper Saddle River, New Jersey.

Hair, J., Black, W., Babin, B., Anderson, R. and Tatham, R. (2006) Multivariate Data Analysis, 6th ed., Pearson Prentice Hall, Upper Saddle River, New Jersey.

Hair, J., Black, W., Babin, B. and Anderson, R. (2010) Multivariate Data Analysis, 7th ed., Pearson Prentice Hall, Upper Saddle River, New Jersey.

Han, S. B., Chen, S. K. and Ebrahimpour, M. (2007) "The Impact of ISO 9000 on TQM and Business Performance", The Journal of Business and Economic Studies, Vol. 13, No. 2, pp. 1-23.

Hartwich, F. (1999) "Weighing of Agricultural Research Results: Strength and Limitations of the Analytical Hierarchy Process (AHP)", <http://www.uni-hohenheim.de/i490a/dps/1999/09-99/dp99-09.pdf>, accessed 03 March 2015.

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.

Hossain, M. F., Adnan, Z. H. and Hasin, A. A. (2014) "Improvement in Weighting Assignment Process in Analytic Hierarchy Process by Introducing Suggestion Matrix and Likert Scale", International Journal of Supply Chain Management, Vol. 3, No. 4, pp. 91-95.

Hult, G. T. M., Boyer, K. K. and Ketchen, D. J. Jr. (2007) "Quality, operational logistics strategy, and repurchase intentions: a profile deviation analysis", Journal

of Business Logistics, Vol. 28, No. 2, pp. 105-132.

Hurley, A. E., Scandura, T. A., Schriesheim, C. A., Brannick, M. T., Seers, A., Vandenberg, R. J. and William, L. J. (1997) “Exploratory and confirmatory factor analysis: guidelines, issues, and alternatives”, Journal of Organizational Behavior, Vol. 18, pp. 667 – 683.

Hwang, H. S., Moon C., Chuang, C. L. and Goan, M. J. (2005) “Supplier Selection and Planning Model Using AHP”, International Journal of the Information Systems for Logistics and Management, Vol. 1, No. 1, pp. 47-53.

ILO (2003) Seafarers’ Identity Documents Convention (Revised), International Labour Organization.

IMB (various years) Piracy and Armed Robbery against Ships, Annual Reports, ICC International Maritime Bureau, web: www.icc-ccs.org.

IMO (1974) The International Convention for the Safety of Life at Sea (SOLAS), International Maritime Organization.

IMO (1988) Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA Convention), International Maritime Organization.

IMO (2002) International Ship and Port Facility Security (ISPS) Code and SOLAS amendments adopted 12 December 2002, International Maritime Organization.

IMO Website www.imo.org, ISPS Code, <http://www.imo.org/ourwork/security/instruments/pages/ispscode.aspx>, accessed 21 February 2015.

Ishizaka, A. and Labib, A. (2009) “Analytic Hierarchy Process and Expert Choice: Benefits and Limitations”, Operational Research Insight, Vol. 22, No. 4, pp. 201–220.

ISO (2000) ISO 9004:2000 Quality management systems Guidelines for performance improvements, International Organization for Standardization.

ISO (2005) ISO 9000:2005 Quality management systems Fundamentals and vocabulary, International Organization for Standardization.

ISO (2007) ISO 28000: 2007 Specification for Security Management System for the Supply Chain, International Organization for Standardization.

Jackson, S. L. (2009) Research Methods and Statistics: A Critical Thinking Approach, 3rd ed., Wadsworth, Belmont, CA.

Jayawardane, A. (2009) “Terrorism at Sea: Maritime Security Challenges in South Asia”, Paper presented at the Third NTS-Asia Annual Convention, 3-4 November, Singapore.

Karlsson, J. and Ryan, K. (1997) “Cost-Value Approach for Prioritizing Requirements”, IEEE Software, September/October 1997, pp. 67-74.

Kim, W., Han, S. K., Oh, K. J., Kim, T. Y., Ahn, H. and Song, C. (2010) “The dual analytic hierarchy process to prioritize emerging technologies”, Technological Forecasting and Social Change, Vol. 77, pp. 566–577.

Kim, W., Kim, B. S. and Youn, M. K. (2012) “Usefulness of analytic hierarchy process (AHP) to determinants win-win growth factor for retailing industry in Korea”, African Journal of Business Management, Vol. 6, No.14, pp. 4824-4834.

Kwang, E. Y. and Youn, C. C. (2006) “Analytic hierarchy process approach for identifying relative importance of factors to improve passenger security checks at airports”, Journal of Air Transport Management, Vol. 12, No. 3, pp. 135–142.

Lambert, D. M. and Harrington, T. C. (1990) “Measuring nonresponse bias in customer service mail surveys”, Journal of Business Logistics, Vol. 11, No. 2, pp. 5-25.

Lee, H. L., and Whang, S. (2005) “Higher supply chain security with lower cost: Lessons from total quality management”, International Journal of Production Economics, Vol. 96, No. 3, pp. 289-300.

Lee, S. and Walsh, P. (2011) “SWOT and AHP hybrid model for sport marketing outsourcing using a case of intercollegiate sport”, Sport Management Review, Vol. 14, pp. 361–369.

Leedy, P. and Omrad, J. (2005) Practical Research, Pearson Prentice Hall, Upper Saddle River, New Jersey.

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.

Mann, R. and Kehoe, D. (1994) “An Evaluation of the Effects of Quality Improvement Activities on Business Performance”, International Journal of Quality and Reliability Management, Vol. 11, No. 4, pp. 29-44.

Markus, M. L. and Robey, D. (1988) “Information Technology and Organizational Change: Causal Structure in Theory and Research”, Management Science, Vol. 34, No. 5, pp. 583-598.

MCA (2008) Mexico 24 Hour Rule, Mexican Customs Authorities.

Metaparti, P. (2010) “Rhetoric, rationality and reality in post-9/11 maritime security”, Maritime Policy and Management, Vol. 37, No. 7, pp. 723-736.

Ministry of Defence, Sri Lanka (2009) Humanitarian Operation – Factual Analysis, July 2006 – May 2009, Ministry of Defence, Democratic Socialist Republic of Sri Lanka, <http://slembassyusa.org/wp-content/uploads/2011/08/Sri-Lankan-Humanitarian-Operation-Factual-Analysis.pdf> , accessed 11 March 2015.

Mohammadi, A. and Ranaei, H. (2011) “The Application of DEA based Malmquist Productivity Index in Organizational Performance Analysis”, International Research Journal of Finance and Economics, No. 62, pp. 68-76.

Moseley, A. (2009) “The Implementation of International Maritime Security Instruments in CARICOM States”, Research Thesis, Division for Ocean Affairs and the Law of the Sea, the Office of Legal Affairs, New York, U.S.

Neely, A., Gregory, M. and Platts, K. (1995) “Performance Measurement System Design: A Literature Review and Research Agenda”, International Journal Operations and Production Management, Vol. 15, No. 4, pp. 80-116.

Nevrous, K. (2010) “Secure supply chain management in a changing world of threats”, Deloitte Service LP, Deloitte Risk Service, [http://www.deloitte.com/assets/Dcom-Australia/Local%20Assets/Documents/Deloitte_Secure_-_supply_chain\(1\).pdf](http://www.deloitte.com/assets/Dcom-Australia/Local%20Assets/Documents/Deloitte_Secure_-_supply_chain(1).pdf), accessed 7 November 2013.

OECD (2004) “The impact of security regulation and other requirement on shippers”, Paper presented at the OECD Workshop on Maritime Transport, 4-5 November, Paris, France.

Onuoha, F. (2009) Sea piracy and maritime security in the Horn of Africa: The Somali coast and Gulf of Aden in perspective, *African Security Review*, 18:3, 31-44, DOI: 10.1080/10246029.2009.9627540.

Palcic, I. and Lalic, B. (2009) “Analytical Hierarchy Process as a Tool for Selecting and Evaluating Projects”, International Journal of Simulation Modelling, Vol. 8, No. 1, pp. 16-26.

Pallis, A. A. and Vaggelas, G. K. (2007) “Enhancing Port Security Via The Enactment Of EU Policies: Operational and economic implications”, In Bell, M., Bichou, K. and Evans, A., Risk Management in Port Operations Logistics and Supply Chain Security, Lloyd’s of London Press, London.

Pallis, A. A. and Vaggelas, G. K. (2008) "Port and Maritime Security: Is there a Distinctive European Approach?" Paper presented at the International Forum on Shipping Ports and Airports (IFSPA), 25-28 May, Hong Kong.

Pallis, T. (2006) "International Ship and Port Facility Security (ISPS) Code and the cost of port compliance", Paper presented at the Maritime Security Forum, October 2006, Piraeus, Greece.

Papa, P. (2013) "US and EU strategies for maritime transport security: A comparative perspective", Transport Policy, No. 28, pp. 75-85.

Park, B. and Kim, R. Y. (2014) "Making a Decision about Importance Analysis and Prioritization of Use Cases through Comparison the Analytic Hierarchy Process (AHP) with Use Case Point (UCP) Technique", International Journal of Software Engineering and Its Applications, Vol.8, No.3, pp.89-96.

Peleg-Gillai, B., Bhat, G. and Sept, L. (2006) "Innovators in Supply Chain Security: Better Security Drives Business Value", The Manufacturing Innovation Series, Stanford University.

Pinar, M. and Girard, T. (2008) "Investigating the Impact of Organizational Excellence and Leadership on Business Performance: an Exploratory Study of Turkish Firms", Advanced Management Journal, Vol. 73, No. 1, pp 29-45.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y. and Podsakoff, N. P. (2003) "Common method biases in behavioral research: A critical review of the literature and recommended remedies", Journal of Applied Psychology, Vol. 88, No. 5, pp. 879-903.

Pristrom, S., Li, K. S., Yang, Z. and Wang, J. (2013) A study of maritime security and piracy, Maritime Policy and Management: The flagship journal of international shipping and port research, Vol. 40, No. 7, pp. 675-693.

Raju, P. S. and Lonial, S. C. (2001) "The impact of quality context and market orientation on organizational performance in a Service Environment", Journal of Service Research, Vol. 4, No. 2, pp. 140-154.

Recker, J. (2011) Evaluations of Process Modelling Grammars, Springer-Verlag, Berlin.

Rice, J. B. Jr., and Spayd, P. W. (2005) “Investing in Supply Chain Security: Collateral Benefits”, Special report series: IBM Center for The Business of Government.

Rice, J. B. Jr. and Tenney, W. (2007) “How risk management can secure your business future”, A newsletter from the MIT Center for Transportation and Logistics, Vol. 3, No. 5, pp. 1-4.

Rice, J. B. Jr., and Caniato, F. (2003a) “Building a Secure and Resilient Supply Network”, Supply Chain Management Review, September/October, pp. 22-30.

Rice, J. B. Jr., and Caniato, F. (2003b) “Supply Chain Response to Terrorism: Creating Resilient and Secure Supply Chains”, Supply Chain Response to Terrorism Project, Interim Report of Progress and Learnings, MIT Center for Transportation and Logistics, U.S.

Richard, P. J., Devinney, T. M., Yip, G. S. and Johnson, G. (2009) “Measuring Organizational Performance: Towards Methodological Best Practice”, Journal of Management, Vol. 35, No. 3, pp. 718-804.

Rietveld, T. & Van Hout, R. (1993) Statistical Techniques for the Study of Language and Language Behaviour, Mouton de Gruyter, Berlin – New York.

Ritter, L. J., Barrett, M. and Wilson, R. (2007) Securing Global Transportation Networks: A Total Security Management Approach, McGraw-Hill, New York.

Roach J. A. (2004) “Initiatives to enhance maritime security at sea”, Maritime Policy, Vol. 28, pp. 41-46.

Rose, K. H. (1995) “A Performance Measurement Method”, Quality Progress, Vol. 28, No. 2, pp. 63-66.

Russell, D. M. and Saldanha, J. P. (2003) “Five tenets of security-aware logistics and supply chain operation”, Transportation Journal, No. 42, Vol. 4, pp. 44-54.

Saaty, T. L. (1977) “A Scaling Method for Priorities in Hierarchical Structures”, Journal of Mathematical Psychology, Vol. 15, pp. 234-281.

Saaty, T. L. (1980) The Analytic Hierarchy Process, McGraw-Hill, New York.

Saaty, T. L. (1994) “Highlights and Critical Points in the Theory and Application of the Analytic Hierarchy Process”, European Journal of Operational Research, Vol. 52, pp. 426-447.

Saaty, T. L. (2000) “On the relativity of relative measures — accommodating both rank preservation and rank reversals in the AHP”, European Journal of Operational Research, Vol. 121, pp. 205–212.

Saaty, T. L. (2008) "Relative Measurement and its Generalization in Decision Making: Why Pairwise Comparisons are Central in Mathematics for the Measurement of Intangible Factors – The Analytic Hierarchy/Network Process", Review of the Royal Academy of Exact, Physical and Natural Sciences, Series A: Mathematics (RACSAM), Vol. 102, No. 2, pp. 251–318.

Saaty, T. L. (2009) Theory and Applications of the Analytic Hierarchy Process, RWS Publications, Pittsburg, PA.

Saaty, T. L. and Özdemir, M. S. (2015) “How Many Judges Should There Be in a Group?”, Annals of Data Science, online publication, DOI 10.1007/s40745-014-0026-4, Published online 11 January 2015.

Sarathy, R. (2006) “Security and the Global Supply Chain”, Transportation Journal, Vol. 45, No 4, pp. 28-51.

Sato, Y. (2004) “Comparison between Multiple-choice and Analytic Hierarchy Process: Measuring Human Perception”, International Transactions in Operational Research, Vol. 11, No. 1, pp. 77-86.

Singapore Customs (2011) Pre-arrival notification and Notification of Arrival (NOA) procedures, Maritime and Port Authority of Singapore, Singapore.

Singapore Customs (2011) Handbook on Secure Trade Partnership, Singapore.

Sheffi, Y. (2001) "Supply chain management under the threat of international terrorism", International Journal of Logistics Management, Vol. 12, No. 2, pp. 1-11.

Sheu, C., Lee, L. and Niehoff, B. (2006) "A voluntary logistics security program and international supply chain partnership", Supply Chain Management: An International Journal, Vol. 11, No. 4, pp. 363-374.

Skrinjar, R., Bosilj-Vuksic, V. and Indihar-Stemberger, M. (2008) "The impact of business process orientation on financial and non-financial performance", Business Process Management Journal, Vol. 14, No. 5, pp. 738-754.

Smith, T. M. and Reece, J. S. (1999) "The relationship of strategy, fit, productivity, and business performance in a services setting", Journal of Operations Management, Vol. 17, No. 2, pp. 145-161.

Stasinopoulos, D. (2003) "Maritime Security - The Need for a Global Agreement", Maritime Economics and Logistics, Vol. 5, No. 3, pp. 311-320.

Talley, W. K. (2008) Maritime safety: security and piracy, Informa, London.

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. (2008) "Service quality in maritime transport: conceptual model and empirical evidence", Asia Pacific Journal of Marketing and Logistics, Vol. 20, No. 4, pp. 493-518.

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.

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.

Thibault, M., R. Brooks, M. and Button, K. J. (2006) “The response of the U.S. Maritime industry to the new container security initiatives”, Transportation Journal, Vol. 45, No. 1, pp. 5-15.

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

Tracey, M., Lim, J. S. and Vonderembse, M. A. (2005) “The impact of supply-chain management capabilities on business performance”, Supply Chain Management, Vol. 10, No. 3/4, pp. 179-191.

Tsai, C. L. (2014) “Asian Seafarers’ Perceptions of Maritime Security Implementation in the Container Shipping Context”, Maritime Quarterly, Vol. 23, No. 1, pp. 87–111.

UNCTAD (2006) “Maritime Security: Elements of an Analytical Framework for Compliance Measurement and Risk Assessment”, Paper presented at the United Nations Conference on Trade and Development, New York and Geneva.

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.

Vargas, L.G. (1990) “An Overview of the Analytic Hierarchy Process and its Applications”, European Journal of Operational Research, No. 48, pp. 2-8.

Vargas, L. G. (2001) “Probabilistic Consideration of the Consistency Index in Reciprocal Matrices”, Proceedings of the International Symposium on the Analytical Hierarchy Process (ISAHP), 2-4 August, Berne, Switzerland.

Venkatraman, N. and Ramanujam, V. (1986) “Measurement of Business Performance in Strategy Research: A Comparison of Approaches”, Academy of Management Review, Vol. 11, No. 4, pp. 801-814.

Voort, M., O'Brien, K. A., Rahman, A. and Valeri, L. (2002) "Seacurity": Improving the Security of the Global Sea-Container Shipping System", RAND Monograph report MR-1695, http://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR1695.pdf, accessed 5 June 2014.

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.

WCO (2007) WCO Safe Framework of Standards, World Customs Organization.

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

Williams, Z., Lueg, J. E. and LeMay, S. A. (2008) "Supply chain security: an overview and research agenda", International Journal of Logistics Management, Vol. 19, No. 2, pp. 254-281.

Williams, Z., Ponder, N. and Autry, C. W. (2009) "Supply chain security culture: measure development and validation", International Journal of Logistics Management, Vol. 20, No. 2, pp. 243-260.

Yamin, S., Gunasekaran, A. and Mavondo, F. T. (1999) "Innovation Index and its Implications on Organizational Performance: A Study of Australian Manufacturing Companies", International Journal of Technology Management, Vol. 17, No. 5, pp. 495-503.

Yang, C. C. and Wei, H. H. (2013) "The effect of supply chain security management on security performance in container shipping operations", Supply Chain Management, Vol. 18, No. 1, pp. 74-85.

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.

Zulkiffli, S. N. A. (2010) “The Impact of Supply Chain Operational Capabilities on Business Performance of Small and Medium Enterprises in Malaysia: A Preliminary Analysis”, International Journal of Business and Management Science, Vol. 3, No. 2, pp. 147-168.

APPENDICES

APPENDIX 1. IN-DEPTH INTERVIEWS

Appendix 1.1. Cover Letter

Dear XXX,

My name is Elena Sadovaya and I am a PhD student at Nanyang Technological University, Singapore. I am writing to seek your help in a research project on the Effective Management of Maritime Security in Shipping Companies. I got your contact details from my supervisor, Asst Prof Thai Van Vinh.

The objective of this project is to propose and validate an effective maritime security management model for shipping companies. For this purpose, we study security management practices implemented in shipping companies and their impacts on organizational performance.

Because of your designation and involvement in maritime security management, I would like to invite you to participate in this research by giving me an opportunity to speak to you in person. Your inputs are important as they will add indispensable information on effective security management in shipping companies. Such inputs will also shed light on how to manage security effectively without jeopardizing organizational performance, which in turn will benefit shipping companies like yours. If you think that somebody else in your company is more familiar with mentioned topic, I would very much appreciate your help in connecting me with your colleagues.

The interview will be focused on your experience about security management practice in your company. However, if a face-to-face interview is not convenient, we can conduct it through telephone if you allow. This research is for academic purpose only. Please be assured that your response will be kept strictly anonymous and confidential. Only aggregate results will be used in the report and will not be linked to any individual or company. As a token of appreciation for your participation, an executive summary of the study will be sent to you if you so wish.

Thank you in advance for your anticipated participation to assist me in my educational endeavours. If you require additional information or have questions, please contact me at elena2@e.ntu.edu.sg / +65 9772 0702 or Asst Prof Thai Van Vinh at vvthai@ntu.edu.sg / +65 6790 5331.

Sincerely,
Elena Sadovaya (Ms)

Appendix 1.2. Interview Information Sheet

Information Sheet for the Interviewees

Research Title

Effective Maritime Security Management in Shipping Companies

Research Background

In the aftermath of the 9/11 event in 2001, maritime security has become one of the main issues on the international maritime agenda, with a strong orientation on anti-terrorism actions. Since that time, a significant number of various regulations in the field of maritime security have come into force. A new security regime has had a noticeable effect on a world maritime industry. Shipping companies face a problem of managing maritime security, since the requirements in this area have a very diverse nature and may jeopardize the organizational performances significantly. Impacts of implementation of security initiatives can differ in similar companies and often depend on approach chosen for security management. Several attempts have been made by researchers to develop models or frameworks for security management. Additionally, some voluntary programs include guidance for supply chain security management. However, the review of related literature shows that some unsolved problems still remain. They include overlapping and inconsistency between the requirements, breaches in maritime security regulations, lack of detailed guidelines for security management, and a need for comprehensive security management framework. Moreover, the main issue for shipping companies is how to manage security effectively without jeopardizing other organizational performance; in other words, how to find a balance between security, resilience and other business performance.

Research Objective

The main objective of this study is to propose and validate an effective maritime security management model for shipping companies.

Interview Enquiries

In this interview we would like to seek your opinion and the experience about two main areas. One area is about maritime security management system in your company. Second area is about changes in your company's performance caused by implementation of security measures.

1. With regard to the security management system in your company we would like you to share your experience about the following aspects:

Aspect of Security Management	Brief Description
1. Security Culture	Security Culture in shipping companies promotes maritime security as a priority among employees through embracing and projecting norms and values that support security-related activities and allow employees to be vigilant in undertaking security-related efforts.
2. Management and Employee Commitment	Management and Employee Commitment helps to involve all of the company's employees into security management according to their responsibilities and positions, it also helps to fill the existing security gaps in the company and make security management more structural.
3. Security Assessment	Security Assessment is essential to understand the current security level in the company, the necessary security level and the measures required to achieve and maintain this level. It also helps to understand the environment in which security threats are derived.
4. Security Policy, System and Procedures	A well-developed and timely reviewed security policy, including security management system and security procedures for all security-related processes and activities in the company, helps to achieve transparency in security management and other security related operations for the company's employees and management.
5. Documentation and Communication	Many of the existing security regulations require shipping companies to collaborate with other participants of the supply chain, as well as with the government for security purposes. The documentation exchange and maintenance is an important part of communication. To secure this area of organizational activities, appropriate security measures should be taken.
6. Process Control	Similarly to quality management, 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 with.
7. Continuous Security Improvement	To achieve the required security level, it is necessary to ensure a constant revision of all security related activities and processes in the company, as well as application of all required follow-up measures.
8. Security Incidents Handling and Continuity of Operations	Security incidents handling and continuity of operations is necessary to mitigate disruptions in the processes in shipping companies. It aims to increase the resilient ability of the company's operations.
9. Business Partners Security	Business Partners Security extends company's security to its suppliers and customers.

2. With regard to your company's performance, we would like you to share your experience about the changes observed from the day of commencement of your company's security system in the following areas:

Company's Performance	Brief Description
1. Security Performance	Security Performance represents a level of security in the company. It can be characterized by numbers of occurred and prevented security incidents, consequences of incidents, level of security related knowledge of company's employees.
2. Business Resilience	Business Resilience shows how well the company can manage crisis (security incident) and continue its operations. It can be describes by time needed for identification, mitigation and recovery from security incidents.
3. Other Business Performance	Other Business Performance includes financial, market, operational and customer performance, and characterizes overall company's efficiency.

Appendix 1.3. Sample of Interview Form

RESEARCH INTERVIEW 3 27/02/2013

1. When was your company's official security system implemented?

- Before 2004 nothing much was implemented for the security purposes, besides the basic security access control. Starting from 2004, we mostly focused on the requirements of the ISPS Code: such as SSP, training of our offices to become CSO, SSO. Besides that not many security measures were implemented. Basically we do not go much outside Singapore. Since Singapore is considered as a very safe port, we only focus on compulsory requirements of the ISPS code.

PART A. COMPONENTS OF THE EFFECTIVE MARITIME SECURITY MANAGEMENT MODEL FOR SHIPPING COMPANIES

A1. What is your overall perception about maritime security management in general and in your company?

- The main problems for security currently are hijacks. That's why presently there's nothing much to be done except the additional security measures. For example for the ships sailing to Dubai we hire armed guards onboard. Of course, some companies think that the cost is hard to be justified. But for us the most important is that our ship reaches Dubai safely, and the cost is quite substantial.

What do you think about the effectiveness of compulsory requirements?

- If we do engage more in the international trade, we would implement the requirements even if they were not mandatory, because currently there're a lot of unsecure activities, but in Singapore there's still safe. Some additional basic measures should be put in place. But as I know Singapore government believe that carrying arms on board are not recommended. But some companies still bring the arms onboard. For us we prefer to hire trained professional security guards.

- But generally, security is not something that can be only implemented by single party or single state; it can only be effective with the cooperation of all the parties and all the states. Currently there're some organizations like ReCAAP, but their purpose is mostly the information dissemination, rather than any actions. But it will not be sufficient in the future, now it's still ok.

- But I believe if you proceed to the area where there're a lot of security incidents, it is due diligence of the ship owner to implement additional measures to secure the ship. If you decide to save money on that, then you put your crew and vessel on risk.

- Generally, I believe that cooperation is required for security management.

A2. In the context of your company, what are the key aspects of maritime security management system?

- We follow strictly the access control requirements. We carry on training of our crew and officers. We supply them with some tools to help them. We carry of the drills, which is the requirement anyway. But the way to carry it very much depends on how high you consider the importance of security. I think in Singapore people are generally quite relax about these things, don't have a high concern. Because the risk in Singapore is not that high, usually only the very minimum level is implemented.

A3. Please refer to page 2 of the Information sheet. Regarding aspects of maritime security management listed in the first table, please share your opinion about implementation and importance of each of them for the effective security management.

Aspect of Security Management	Responses
1. Security Culture	-We only keep the minimum requirements and comply with requirements of our customers.
2. Management and Employee Commitment	- Pretty much standard. We always rely quite heavily on government what to do. - - We don't have any dedicated team to manage security. What we do is just telling our employees what to do. However there're still violations of security rules, and usually employees are not punished for that. But if the violation is severe we fire the responsible personnel. - Also we implement additional control measures for the crew when it's necessary.
3. Security Assessment	- There're several trading routs we try to avoid. Besides that we do consider reports about incidents before planning the rout. However, not much more is done for security assessment, because the risk is low.
4. Security Policy, System and Procedures	- They're important, but you always need to consider how relevant they are. It doesn't affect much if the policy is detailed or not. - Pretty much basic implementation. They are in place, but not very detailed. - We do have procedures for the screening of employees. But the screening is not really for security purposes, but overall screening.
5. Documentation and Communication	- We do share some information with other companies. - Generally we rely heavily on government in terms of sharing the information about accidents. - But we have system backups.
6. Process Control	- Because our company is small we do not pay much attention to it. But probably in bigger companies the process control is more exercised. We installed CCTV onboard the ships. Also our superintendant visits a ship every month.
7. Continuous Security Improvement	- Generally, we review the SSP on the regular basis. We also review the environment.
8. Security Incidents Handling and Continuity of Operations	- We do have some plans, but we don't have any special team. Because generally the team is not able to do much in case of the major incident. We also implement BCM but it's mostly because our customers require that. We're certified with BCM: remote server location, backups, disaster recovery plans, and exercises.
9. Business Partners Security	- There's no specific procedure for screening of proposed suppliers. We have a list of recognized suppliers with who we usually work. But we do not screen much, however the assessment of them is done during mutual projects. Security wise we don't do screening. - Our customers are usually big companies and they have a procedures and requirements for their suppliers. So we have to comply with them.

- When it comes to security more investments should be done to the international shipping companies. So far we don't leave the region. So we do comply, we do carry on some initiatives, but the culture in other shipping companies is different from our tanker company. The culture of our company is that we focus mostly on mandatory requirements. Additionally our partners, big oil companies, have slightly higher security requirements. That's why we always need to comply with what they require from us, because they're our customers who pays for the equipment.
- If you look at security, usually it's quite high operating cost but the actual operation level is very low, there's not much the company can do.

A4. Is there anything else that should be improved besides the nine aspects above?

- We operate in a relatively safe region that's why the concern is not so high. And we also don't want to bring many resources when it's not necessary.

PART B. PERFORMANCE OF SHIPPING COMPANIES

B1. We would like you to share your experience about your company's performance. Since the first day of implementation of security management system, have you observed any changes in your company performance?

- Onboard of our ships so far there were no accidents. But we did have cases when the crew stole the cargo and sell it. And then they were caught.

B2. Please refer to page 2 of the Information Sheet. Besides changes mentioned above, please indicate if you have observed any changes in following performance, if these changes are negative or positive, and to what extend they have been observed?

Company's Performance	Changes
1. Security Performance	<ul style="list-style-type: none"> - Our vessels were always quite secure, because the risk level is quit low. - Awareness is there however due to our environment it's taken for granted. Of course we still know that anything can happen, that's why we still remind them that the accidents can happen, we do distribute some information. - But in terms of real physical activity there's no experience.
2. Business Resilience	<ul style="list-style-type: none"> - Actually there's zero experience in this company due to security. But at the office context we recently got certified for BCM. That is at least little additional standards we've taken to assure that we are still able to operate within any circumstances. BCM consultancy is carried out by third party. They helped us to assess what are the requirements, what we need to do. Part of the cost for this certification is reimbursed by government. We also try to use this certification to attract the customers.
3. Other Business Performance	<ul style="list-style-type: none"> - For bunker suppliers in Singapore the focus is not much on security. The only requirement is that in case if any event happens the company will be still able to operate. - Business wise we are one of the reputable suppliers in bunker industry. - The competitiveness can be lower because of the price, but branding is depending on what customers prefer. Our customers usually prefer better reputation and reliability to the price. - Customer satisfaction. - The main negative impact is price. It's always about how much you can price yourself. But your security readiness is higher that other companies have. But usually if you do it in an every day basis, the price is lower. If you plan and do a full-scale assess, than the price can be lower. But still when you plan you find new areas where the investments are necessary, but if you don't really plan you don't see these gaps.

PART C. CLASSIFYING INFORMATION

C1. Interviewee's experience (years) in the security related job:

- 6-7 years ashore, 2 years in the company as CSO, DPA.

C2. Please indicate your main trading area:

- 11 tankers, Singapore - Malaysia, Dubai

C3. May I send you a questionnaire?

- yes

C4. Could you please refer me to other people who have an experience in maritime security management?

-

C5. Would you like to receive a copy of this report?

- yes

If yes, please indicate your e-mail address for correspondence:

The email address will not be shared to another party.

APPENDIX 2. MAIN SURVEY

Appendix 2.1. Sample of Questionnaire Pre-test Form

Dear Sir/Madam,

Thank you very much for taking time to help me in the pre-testing of the questionnaire. As the purpose of reviewing the questionnaire is to improve on it, I appreciate your comments. Please indicate *(by choosing the most appropriate number)* your opinion on the questionnaire by completing the table below:

No.		Strongly Disagree			Strongly Agree		If you have chosen answers 1, 2 or 3, please specify the question(s) or section(s) of your concern
		1	2	3	4	5	
1	I understand the objective of each part in the questionnaire.				X		N.A.
2	The questions in each part of the questionnaire are appropriate to measure their intended objective.					X	N.A.
3	I could follow the layout of the questionnaire easily.					X	N.A.
4	The length of the questionnaire is appropriate.			X			Personally I thought its quite long questionnaire, especially when you are into the subject and have to fill in all the boxes, but I understand its for research purposes
5	The instructions in the questionnaire are easy to follow.				X		I would prefer more shorter and crisper descriptions
6	I did not have to think too long when answering the questions.				X		N.A.
7	The wordings of the questions are concise.				X		N.A.
8	The wordings of the questions are clear.				X		N.A.
9	The questions are easy to understand.				X		N.A.
10	The questions asked did not make me feel uncomfortable, irritated or embarrassed.					X	N.A.
11	There is only one intended query in each question.				X		N.A.
12	The questions asked did not hint me to answer in a particular way.					X	N.A.

Comments and suggestions:

Very good questionnaire, easy to follow and read. On the improvement sides maybe make it more shorter and crisp in terms of introduction text, and if possible, make it slightly shorter.

Appendix 2.2. Cover Letter

Dear Sir/Madam,

My name is Elena Sadovaya and I am a PhD student at Nanyang Technological University, Singapore. I am writing to seek your help in a research project on the effective management of maritime security in shipping companies. The objective of this project is to propose and validate an effective maritime security management model for shipping companies. For this purpose, we study security management practices implemented in shipping companies and their impacts on organizational performance.

Because of your designation and involvement in maritime security management, I would like to invite you to participate in this research study by completing the attached questionnaire. Your inputs are important, as they will add indispensable information on effective security management in shipping companies. Such inputs will also shed light on how to manage security effectively without jeopardizing organizational performance, which in turn will benefit companies like yours.

I would greatly appreciate if you could spare some of your valuable time to participate in this survey. Please answer all questions as honestly as possible. Kindly send the completed questionnaires back to us by Email to elena2@e.ntu.edu.sg before **8th August 2013**. Alternatively you may wish to fill the online questionnaire by clicking the link: <http://edu.surveymizmo.com/s3/1253065/Study-of-the-Effective-Maritime-Security-Management>. This research is for academic purpose only. Please be assured that your response will be kept strictly anonymous and confidential. Only aggregate results will be used in the report and will not be linked to any individual or company. As a token of appreciation for your participation, an executive summary of the study will be sent to you if you so wish.

If you're not a person responsible for maritime security management in your company, please kindly pass this email to your colleague who is more familiar with this topic.

Thank you in advance for your participation and assistance in my educational endeavours. If you require additional information or have questions, please contact me at elena2@e.ntu.edu.sg / +65 9772 0702 or Asst Prof Thai Van Vinh at vvthai@ntu.edu.sg / +65 6790 5331.

Sincerely,
Elena Sadovaya (Ms)

Appendix 2.3. Reminder Letter

Dear Sir/Madam,

This is a gentle reminder to participate in our survey for the research project entitled '*Study of the Effective Management of Maritime Security in Shipping Companies*' conducted by Nanyang Technological University of Singapore. If you have already completed and returned the questionnaire, we would like to thank you very much for your contribution to this research. However, if you have not yet responded, we would highly appreciate if you do so since your response is extremely important to our study. Please find attached with this letter the questionnaire for your kind input. The survey will be closed on **17 September 2013**. Please kindly return the questionnaire to us by that day. Alternatively you may wish to fill the online questionnaire by clicking the link: <http://edu.surveymzmo.com/s3/1253065/Study-of-the-Effective-Maritime-Security-Management>

To thank you for your help in participating in our study, a summary of results will be sent to you if you so wish, by checking the box at the end of the questionnaire.

Should you have questions or desire additional information, please feel free to contact the following researcher:

PhD Student Elena Sadovaya at elena2@e.ntu.edu.sg / +65 9772 0702 or
Asst Prof Thai Van Vinh at vvthai@ntu.edu.sg / +65 6790 5331.

Sincerely,
Elena Sadovaya (Ms)

Appendix 2.4. Samples of Questionnaire

Appendix 2.4.1. Questionnaire in Word document

Next four pages show the filled questionnaire.

Study of the Effective Maritime Security Management

1. This questionnaire contains three parts. Part A is about effective maritime security management model for shipping companies. Part B studies the impacts of implementation of security regulations on organizational performance. Part C seeks to obtain demographic information.

2. There is no right or wrong answer. Please choose the response that most represents your perception. If you are not sure about particular question area, please feel free to consult a colleague of you in that area.

3. **‘Effective maritime security management’** can be described as *an essential and integrated part of overall organizational management, focusing on the coordination of activities, the implementation of compulsory and voluntary security requirements, as well as other security related activities, for the purpose of managing security related risks inside and outside the organization while enhancing organizational performance at the same time.*

Part A. Components of the Effective Maritime Security Management Model

1. With regard to security management **in your company**, please select an appropriate answer on the below scale to indicate the extent to which you agree or disagree with each of the following statements.

No.	Components of Effective Security Management	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
A1	Security Culture					
A1.1	Senior management promotes security as an essential part of every day organizational activity.	☐	☐	☐	☒	☐
A1.2	Security issues are included in the agendas of scheduled management meetings.	☐	☐	☐	☒	☐
A1.3	Training seminars and courses on maritime security are conducted <u>for managers</u> .	☐	☐	☒	☐	☐
A1.4	Security trainings, drills, exercises and seminars are periodically conducted <u>for employees</u> .	☐	☐	☒	☐	☐
A1.5	Security information is periodically distributed among employees by email, posters, videos, etc.	☐	☐	☐	☒	☐
A2	Management and Employee Commitment					
A2.1	Security related roles and responsibilities are clearly identified and documented for employees.	☐	☐	☒	☐	☐
A2.2	The procedures for security related decision making are clearly identified and documented.	☐	☐	☒	☐	☐
A2.3	Senior management considers security investments as a service quality improvement facilitator.	☐	☐	☒	☐	☐
A2.4	Senior management allocates adequate resources (<i>financial, human, etc.</i>) for security improvement.	☐	☐	☒	☐	☐
A2.5	Employees from different levels are involved in processes of security related decision making.	☐	☒	☐	☐	☐
A2.6	Procedures for employees to report security errors and breaches are established.	☐	☐	☒	☐	☐
A2.7	A platform for employees to propose necessary changes and possible solutions is established.	☐	☒	☐	☐	☐
A2.8	Reward & Recognition program is established to motivate employees to provide security feedback.	☒	☐	☐	☐	☐
A3	Security Assessment					
A3.1	The internal security audit of all activities and departments is periodically conducted.	☐	☒	☐	☐	☐
A3.2	Security related risks are periodically identified.	☐	☐	☒	☐	☐
A3.3	Security risk assessment is conducted to derive a risk magnitude.	☐	☐	☒	☐	☐
A3.4	Risk acceptance levels are established based on risk magnitudes and existing control barriers.	☐	☐	☒	☐	☐
A3.5	Measures are implemented to mitigate identified risks according to risk acceptance levels.	☐	☐	☒	☐	☐
A3.6	Investments in security are made according to risk magnitude and risk acceptance levels (<i>investments in security facilities, equipment, manpower, etc.</i>).	☐	☐	☒	☐	☐
A3.7	<u>All prospective employees</u> periodically go through background screening for security purposes.	☐	☐	☐	☒	☐
A3.8	A background screening of <u>all current employees</u> is periodically conducted for security purposes.	☐	☒	☐	☐	☐

A4		Security Policy, System and Procedures				
A4.1	A well-structured security management policy is developed and documented.	☐	☒	☐	☐	☐
A4.2	Security management policy includes security management system, procedures, plans, etc.	☐	☒	☐	☐	☐
A4.3	Security policy is included into overall company policy.	☐	☒	☐	☐	☐
A4.4	Security policy, system, procedures, plans do not contradict with other measures and procedures.	☒	☐	☐	☐	☐
A4.5	Security measures are integrated into daily activities.	☒	☐	☐	☐	☐
A5		Documentation and Communication				
A5.1	A communication system is established with authorities, partners, agents, etc. for security purposes.	☐	☐	☒	☐	☐
A5.2	Detailed procedures for security communication are developed and documented.	☐	☒	☐	☐	☐
A5.3	Data and processes in the communication system are periodically backed up.	☐	☐	☒	☐	☐
A5.4	Measures to secure organizational documentation and information are developed and implemented.	☐	☐	☒	☐	☐
A5.5	Documentation and information systems are periodically backed up.	☐	☐	☐	☒	☐
A5.6	IT security measures are implemented.	☐	☐	☐	☒	☐
A6		Process Control				
A6.1	Management promotes the idea of security prevention by making it right from the first time.	☐	☐	☒	☐	☐
A6.2	A measurement system is developed and put in place to monitor and review all security processes.	☐	☒	☐	☐	☐
A6.3	A proofreading system is used to detect security loopholes and implement corrections immediately.	☒	☐	☐	☐	☐
A6.4	Tracking and tracing technologies are implemented for commercial and security purposes.	☐	☐	☐	☒	☐
A6.5	Procedures for detection and response to security incidents are clearly defined and documented.	☐	☒	☐	☐	☐
A6.6	Investments in technologies, software and/or equipment are made to improve access control.	☐	☐	☒	☐	☐
A7		Continuous Security Improvement				
A7.1	Security procedures are constantly reviewed and improved according to security requirements.	☐	☐	☒	☐	☐
A7.2	Security targets, methods and a time line are clearly established and documented.	☐	☐	☒	☐	☐
A7.3	Corrective actions and removal of the root cause of security errors are timely undertaken.	☒	☐	☐	☐	☐
A7.4	We conduct research on security improvement and/or participate in similar projects.	☐	☒	☐	☐	☐
A8		Security Incidents Handling and Continuity of Operations				
A8.1	We consider and predict all various scenarios of maritime security threats.	☐	☐	☒	☐	☐
A8.2	Disaster, crisis management and emergency plans are developed based on considered scenarios.	☐	☐	☒	☐	☐
A8.3	Training and drills on disaster and crisis management are periodically conducted.	☐	☐	☒	☐	☐
A8.4	Recovery and business continuity plans are developed and reviewed.	☐	☒	☐	☐	☐
A8.5	Training and drills on recovery and business continuity management are periodically conducted.	☐	☐	☒	☐	☐
A8.6	Dedicated communication channels exist for emergency cases.	☐	☐	☒	☐	☐
A9		Business Partners Security				
A9.1	All future business partners undergo security background checks.	☐	☐	☒	☐	☐
A9.2	All current partners are periodically assessed to ensure their compliance with security requirements.	☐	☒	☐	☐	☐
A9.3	Security trainings and exercises are jointly organized with business partners.	☐	☐	☒	☐	☐
A9.4	Collaboration with business partners exists to identify, mitigate and share security risks.	☐	☐	☒	☐	☐
A9.5	Liabilities for possible security incidents are clearly defined in contracts with business partners.	☐	☐	☒	☐	☐

2. Please identify other factors, which are not listed above, but implemented as a part of the security management system in your company.

FACTORS ARE COMPREHENSIVELY COVERED.

Part B. Organizational Performance

1. Please select an appropriate answer on the below scale to indicate the changes in **your company's performance** from the day of commencement of the security management system. Please choose the "N/A" option if you are not able to give an answer about the indicator.

No.	Performance Indicators	Significantly decrease	Decrease	Same as before	Increase	Significantly increase	N/A
B1	Security Performance						
B1.1	Number of cargo pilferage (cases)	☐	☐	☐	☐	☒	☐
B1.2	Number of stowaways (cases)	☐	☐	☐	☐	☒	☐
B1.3	Number of ship attacks, including terrorist and piracy attack, armed robbery (cases)	☐	☐	☐	☒	☐	☐
B1.4	Number of tampering with cargo, data and physical shipment (cases)	☐	☐	☐	☒	☐	☐
B1.5	Cargo loss and damage (dollars)	☐	☐	☐	☐	☒	☐
B1.6	Number of smuggling (cases)	☐	☐	☐	☒	☐	☐
B1.7	Number of violations of security rules by employees (cases)	☐	☐	☒	☐	☐	☐
B1.8	Number of prevented security incidents (cases)	☐	☒	☐	☐	☐	☐
B1.9	Level of employees' knowledge on security requirements, measures, threats, risks, etc.	☐	☐	☒	☐	☐	☐
B2	Business Resilience						
B2.1	Time taken to identify security problems	☐	☐	☒	☐	☐	☐
B2.2	Time taken to mitigate security problems	☐	☒	☐	☐	☐	☐
B2.3	Time taken to recover from security incidents	☐	☒	☐	☐	☐	☐
B2.4	Customer service level during disruption compared to normal operation time	☐	☐	☒	☐	☐	☐
B3	Other Business Performance						
B3.1	Total cost per TEU or per ton	☐	☐	☐	☒	☐	☐
B3.2	Profit margin per TEU or per ton	☐	☐	☐	☒	☐	☐
B3.3	Level of competitiveness	☐	☐	☐	☐	☒	☐
B3.4	Level of reputation for liability	☐	☐	☐	☒	☐	☐
B3.5	Level of market share	☐	☐	☐	☐	☒	☐
B3.6	Vessels' port turnaround time	☐	☐	☐	☐	☒	☐
B3.7	Vessels' total voyage time	☐	☐	☐	☐	☒	☐
B3.8	Vessels' schedule delays because of security issues	☐	☐	☐	☒	☐	☐
B3.9	Number of Port State Control inspections on your company's vessels	☐	☐	☐	☐	☒	☐
B3.10	Additional cost because of security issues	☐	☐	☐	☐	☒	☐
B3.11	Level of business process's interruptions	☐	☐	☐	☒	☐	☐
B3.12	Level of use of track and trace system	☐	☐	☐	☒	☐	☐
B3.13	Level of on-time delivery of cargo	☐	☐	☐	☒	☐	☐
B3.14	Level of documentation accuracy	☐	☒	☐	☐	☐	☐
B3.15	Level of flexibility in responding to customer requests	☐	☒	☐	☐	☐	☐
B3.16	Level of customers' overall satisfaction about physical resources	☒	☐	☐	☐	☐	☐
B3.17	Level of customers' overall satisfaction about quality of service provided	☐	☒	☐	☐	☐	☐
B3.18	Number of new customers	☐	☐	☐	☒	☐	☐
B3.19	Number of repeated customers	☐	☐	☐	☒	☐	☐

2. Please name other changes in the performance of your company if they are not listed above.

NONE TO ADD AS PERFORMANCE IS WELL COVERED

Part C. Demographic information

1. Your designation: **GENERAL MANAGER**

2. Number of years in the security related job or industry: **5**

3. Your business sector:

☒ Shipping Company. *Please indicate the types of vessels your company operates:*

☒ general cargo	☒ tanker
☒ containership	☒ others:
☒ bulk carrier	

☒ Ship Management Company. *Please indicate the types of vessels your fleet includes:*

☐ general cargo	☒ tanker
☐ containership	☒ others:
☒ bulk carrier	

Also, please indicate what type of management your company provides to ship owners:

☒ technical management	☐ commercial management
☒ crew management	☐ others:

☐ Others (*Please specify*)

4. Please indicate the trading areas of your company's vessels:

☒ Worldwide	☐ Europe	☐ Middle East
☐ Asia	☐ North America	☐ Africa
☐ Oceania	☐ South America	

5. In what country is your office located? **SINGAPORE AND INDONESIA + 37 LOCATIONS ON A WORLDWIDE BASIS.**

6. Should you wish to receive the executive summary of this research, please indicate your e-mail address for correspondence. The email address will not be shared with another party.

~Thank you very much for your valuable contribution to this study~

Appendix 2.4.2. Online Questionnaire

Next five pages show the filled questionnaire.

Study of the Effective Maritime Security Management

Response ID:80 Data

2. Page 2 of 4

1. Security Culture

	1	2	3	4	5
Senior management promotes security as an essential part of every day organizational activity.				✓	
Security issues are included in the agendas of scheduled management meetings.				✓	
Training seminars and courses on maritime security are conducted for managers.				✓	
Security trainings, drills, exercises and seminars are periodically conducted for employees.				✓	
Security information is periodically distributed among employees by email, posters, videos, etc.					✓

2. Management and Employee Commitment

	1	2	3	4	5
Security related roles and responsibilities are clearly identified and documented for employees.				✓	
The procedures for security related decision making are clearly identified and documented.					✓
Senior management considers security investments as a service quality improvement facilitator.				✓	
Senior management allocates adequate resources (financial, human, etc.) for security improvement.			✓		
Employees from different levels are involved in processes of security related decision making.			✓		
Procedures for employees to report security errors and breaches are established.				✓	
A platform for employees to propose necessary changes and possible solutions is established.				✓	
Reward & Recognition program is established to motivate employees to provide security feedback.		✓			

3. Security Assessment

	1	2	3	4	5
The internal security audit of all activities and departments is periodically conducted.				✓	
Security related risks are periodically identified.				✓	
Security risk assessment is conducted to derive a risk magnitude.				✓	
Risk acceptance levels are established based on risk magnitudes and existing control barriers.				✓	
Measures are implemented to mitigate identified risks according to risk acceptance levels.				✓	
Investments in security are made according to risk magnitude and risk acceptance levels (investments in security facilities, equipment, manpower, etc.).			✓		
All prospective employees periodically go through background screening for security purposes.		✓			
A background screening of all current employees is periodically conducted for security purposes.		✓			

4. Security Policy, System and Procedures

	1	2	3	4	5
A well-structured security management policy is developed and documented.				✓	
Security management policy includes security management system , procedures, plans, etc.				✓	
Security policy is included into overall company policy.				✓	
Security policy, system , procedures, plans do not contradict with other measures and procedures.				✓	
Security measures are integrated into daily activities.				✓	

5. Documentation and Communication

	1	2	3	4	5
A communication system is established with authorities, partners, agents, etc. for security purposes.				✓	
Detailed procedures for security communication are developed and documented.				✓	
Data and processes in the communication system are periodically backed up.				✓	
Measures to secure organizational documentation and information are developed and implemented.				✓	
Documentation and information systems are periodically backed up.				✓	
IT security measures are implemented.				✓	

6. Process Control

	1	2	3	4	5
Management promotes the idea of security prevention by making it right from the first time.				✓	
A measurement system is developed and put in place to monitor and review all security processes.				✓	
A proofreading system is used to detect security loopholes and implement corrections immediately.			✓		
Tracking and tracing technologies are implemented for commercial and security purposes.				✓	
Procedures for detection and response to security incidents are clearly defined and documented.					✓
Investments in technologies, software and/or equipment are made to improve access control.			✓		

7. Continuous Security Improvement

	1	2	3	4	5
Security procedures are constantly reviewed and improved according to security requirements.				✓	
Security targets, methods and a time line are clearly established and documented.			✓		
Corrective actions and removal of the root cause of security errors are timely undertaken.				✓	
We conduct research on security improvement and/or participate in similar projects.				✓	

8. Security Incidents Handling and Continuity of Operations

	1	2	3	4	5

We consider and predict all various scenarios of maritime security threats.				✓	
Disaster, crisis management and emergency plans are developed based on considered scenarios.				✓	
Training and drills on disaster and crisis management are periodically conducted.				✓	
Recovery and business continuity plans are developed and reviewed.			✓		
Training and drills on recovery and business continuity management are periodically conducted.			✓		
Dedicated communication channels exist for emergency cases.				✓	

9. Business Partners Security

	1	2	3	4	5
All future business partners undergo security background checks.			✓		
All current partners are periodically assessed to ensure their compliance with security requirements.				✓	
Security trainings and exercises are jointly organized with business partners.			✓		
Collaboration with business partners exists to identify, mitigate and share security risks.				✓	
Liabilities for possible security incidents are clearly defined in contracts with business partners.				✓	

2. Please identify other factors, which are not listed above, but implemented as a part of the security management system in your company.

3. Page 3 of 4

1. Security Performance

	1	2	3	4	5	NA
Number of cargo pilferage (cases)						✓
Number of stowaways (cases)						✓
Number of ship attacks, including terrorist and piracy attack, armed robbery (cases)						✓
Number of tampering with cargo, data and physical shipment (cases)						✓
Cargo loss and damage (dollars)						✓
Number of smuggling (cases)						✓
Number of violations of security rules by employees (cases)						✓
Number of prevented security incidents (cases)				✓		
Level of employees' knowledge on security requirements, measures, threats, risks, etc.				✓		

2. Business Resilience

	1	2	3	4	5	NA
Time taken to identify security problems			✓			
Time taken to mitigate security problems				✓		

Time taken to recover from security incidents					✓		
Customer service level during disruption compared to normal operation time			✓				

3. Other Business Performance

	1	2	3	4	5	NA
Total cost per TEU or per ton			✓			
Profit margin per TEU or per ton			✓			
Level of competitiveness			✓			
Level of reputation for liability			✓			
Level of market share			✓			
Vessels' port turnaround time						✓
Vessels' total voyage time						✓
Vessels' schedule delays because of security issues						✓
Number of Port State Control inspections on your company's vessels			✓			
Additional cost because of security issues						✓
Level of business process's interruptions						✓
Level of use of track and trace system			✓			
Level of on-time delivery of cargo						✓
Level of documentation accuracy			✓			
Level of flexibility in responding to customer requests			✓			
Level of customers' overall satisfaction about physical resources				✓		
Level of customers' overall satisfaction about quality of service provided				✓		
Number of new customers			✓			
Number of repeated customers			✓			

2. Please name other changes in the performance of your company if they are not listed above.

4. Page 4 of 4

1. Your designation

junior fleet manager

2. Number of years in the security related job or industry

5

3. Your business sector

Others

Please indicate the types of vessels your company operates

Please indicate the types of vessels your fleet includes

Also, please indicate what type of management your company provides to ship owners

Please specify

Yacht Management

Please indicate the trading areas of your company's vessels

4. Please indicate the country, where your office is located.

France

5. Should you wish to receive the executive summary of this research, please indicate your e-mail address for correspondence. The email address will not be shared with another party.

5. Thank You!

Send Email to Me

Jul 29, 2013 05:52:17 Success: Email Sent to: elena2@e.ntu.edu.sg

Send Email

Jul 29, 2013 05:52:17 Skipped: No emails

Response Location

Country:	France
Region:	
City:	
Postal Code:	
Long & Lat:	Lat: 46, Long:2

APPENDIX 3. CONFIRMATORY SURVEY

Appendix 3.1. Cover Letter

Dear Survey Participant,

We would like to thank you again for your valuable participation in our recent survey on the effective management of maritime security in shipping companies. The survey was successfully conducted and the results were statistically analyzed. To further confirm these results, we would like to conduct a short confirmatory survey. We would greatly appreciate if you could spare some of your valuable time to participate in this study again. It will take 5-10 minutes to fill in the questionnaire.

Kindly send the completed questionnaires back to us by email to elena2@e.ntu.edu.sg before **21st February 2014**. This research is for academic purpose only. Please be assured that your response will be kept strictly anonymous and confidential. Only aggregate results will be used in the report and will not be linked to any individual or company. As a token of appreciation for your participation, an executive summary of the study will be sent to you if you so wish.

Thank you in advance for your participation and assistance in my educational endeavours. If you require additional information or have questions, please contact me at elena2@e.ntu.edu.sg / +65 9772 0702 or Asst Prof Thai Van Vinh at vvthai@ntu.edu.sg / +65 6790 5331.

Sincerely,
Elena Sadovaya (Ms)

Appendix 3.2. Sample of Questionnaire

Next four pages show the filled questionnaire.

Study of Effective Maritime Security Management in Shipping Companies

1. This survey contains four sections. Section A provides a short description of the factors of the Effective Maritime Security Management Model. Section B explains how to answer the questions. Section C seeks to explore respondents' perception of the relative importance of the factors, while Section D is about respondents' demographic information.

2. **'Effective maritime security management'** can be described as *an essential and integrated part of overall organizational management, focusing on the coordination of activities, the implementation of compulsory and voluntary security requirements, as well as other security related activities, for the purpose of managing security related risks inside and outside the organization while enhancing organizational performance at the same time.*

A. Factors of the Effective Maritime Security Management Model for Shipping Companies

Factors	Description	Attributes
<i>Management and Employee Commitment</i>	Helps to involve all employees into security management according to their responsibilities and positions. Helps to fill the existing security gaps in a company and make security management more structural.	1. Senior management promotes security as an essential part of everyday activity. 2. A platform for employees to propose necessary changes is established.
<i>Security Assessment</i>	Helps to understand the current security level in a company, the necessary security level and the measures required to achieve and maintain this level. Helps to understand the environment in which security threats are derived.	1. Security risk assessment is conducted to derive a risk magnitude. 2. Risk acceptance levels are established based on risk magnitudes and control barriers. 3. Measures are implemented to mitigate identified risks according to risk acceptance levels.
<i>Security Policy, System and Procedures</i>	Should be developed for all security-related processes and activities. Helps to achieve transparency in security management and other security related operations for the company's employees and management.	1. A well-structured security management policy is developed and documented. 2. Security management policy includes security management system, procedures, plans, etc. 3. Security policy is included into overall company policy. 4. Security policy, system, procedures do not contradict with other measures and procedures.
<i>Documentation and Communication</i>	Helps to secure documentation exchange and maintenance. Helps to secure communication and collaboration with other participants of the supply chain, as well as with the government for security purposes.	1. Data and processes in the communication system are periodically backed up. 2. Measures to secure organizational documentation and information are implemented. 3. Documentation and information systems are periodically backed up. 4. IT security measures are implemented.
<i>Security Incidents Handling and Continuity of Operations</i>	Helps to mitigate disruptions in the processes in shipping companies. Aims to increase the resilient ability of company's operations.	1. Disaster, crisis management and emergency plans are developed. 2. Training and drills on disaster and crisis management are periodically conducted.
<i>Business Partners Security</i>	Helps to extend security to company's suppliers and customers.	1. Future business partners undergo security background checks. 2. Partners are periodically assessed to ensure their compliance with security requirements. 3. Security trainings and exercises are jointly organized with business partners. 4. Collaboration with business partners exists to identify, mitigate and share security risks. 5. Liabilities for possible security incidents are clearly defined in contracts with partners.

B. Explanation and Examples of Terms and Scales Used

1. Scale of Relative Importance:

Intensity of Relative Importance	Definition
1	Equal Importance
2	Equal to Moderate Importance
3	Moderate Importance of one over another
4	Moderate to Strong Importance
5	Essential or Strong Importance
6	Strong to Demonstrated Importance
7	Demonstrated Importance
8	Demonstrated to Extreme Importance
9	Extreme Importance

2. Examples of Terms of Scales Used:

- If you think “Security Assessment” is 9 times more important than “Business Partners Security” for the effective management of maritime security, please cross as follows:

Criterion	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Criterion
Security Assessment	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Business Partners Security

In this case, crossing 9 means you think “Security Assessment” has **extreme importance** for security management to “Business Partners Security”.

- If you think “Business Partners Security” is 9 times important than “Security Assessment” for the effective management of maritime security, please cross as follows:

Criterion	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Criterion
Security Assessment	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☒	Business Partners Security

In this case, crossing 9 means you think “Business Partners Security” has **extreme importance** for security management to “Security Assessment”.

C. Importance of the Factors of the Effective Maritime Security Management Model

Criterion	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Criterion
Management and Employee Commitment	☐	☐	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Business Partners Security
Security Assessment	☐	☐	☐	☐	☐	☐	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	Security Incidents Handling and Continuity of Operations
Security Policy, System and Procedures	☐	☐	☐	☐	☐	☐	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	Documentation and Communication
Business Partners Security	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☒	☐	☐	Security Assessment
Security Incidents Handling and Continuity of Operations	☐	☐	☐	☐	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Management and Employee Commitment
Documentation and Communication	☐	☐	☐	☐	☐	☐	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	Security Assessment
Security Policy, System and Procedures	☐	☐	☐	☐	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Management and Employee Commitment
Security Assessment	☐	☐	☐	☐	☐	☐	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	Security Policy, System and Procedures
Management and Employee Commitment	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☒	☐	☐	☐	☐	☐	☐	Documentation and Communication
Security Incidents Handling and Continuity of Operations	☐	☐	☐	☐	☐	☐	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	Security Policy, System and Procedures
Business Partners Security	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☒	☐	☐	☐	☐	Documentation and Communication
Management and Employee Commitment	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☒	☐	☐	Security Assessment
Security Policy, System and Procedures	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Business Partners Security
Documentation and Communication	☐	☐	☐	☐	☐	☐	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	Security Incidents Handling and Continuity of Operations
Security Incidents Handling and Continuity of Operations	☐	☐	☐	☐	☐	☐	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	Business Partners Security

D. Demographic Information

1. Your designation:

Company's Vice-President

2. Please indicate the trading areas of your company's vessels:

☒ Europe

☐ Asia

☐ Oceania

☐ Africa

☐ Middle East

☐ North America

☐ South America

3. As a token of appreciation for your participation, an executive summary of the study will be sent to you once it is ready.

Please indicate if you would like to have the document sent to a different email address:

~Thank you very much for your valuable contribution to this study~

Appendix 3.3. Matrix Resulted from the Questionnaire

The below matrix was constructed based on the responses provided in the questionnaire, shown in Appendix 3.2.

	COMMIT	ASSES	PROCED	DOCUM	INCID	PARTNERS
COMMIT	1.00	0.14	0.33	0.33	0.33	5.00
ASSES	7.00	1.00	1.00	1.00	1.00	7.00
PROCED	3.00	1.00	1.00	1.00	1.00	7.00
DOCUM	3.00	1.00	1.00	1.00	1.00	5.00
INCID	3.00	1.00	1.00	1.00	1.00	1.00
PARTNERS	0.20	0.14	0.14	0.20	1.00	1.00

Appendix 3.4. Results of the Confirmatory (AHP) Survey

The below table shows the consistency ratios (C.R.) and harmonized weights for each of nine matrices, their average consistency ratio, as well as their geometric average and percentage.

Factors compared	Harmonized Weights									Harmonized Weights, Geometric Average	Percentage, %
	1	2	3	4	5	6	7	8	9		
COMMIT	0.33	0.14	0.14	0.27	0.25	0.08	0.29	0.13	0.08	0.17	20
INCID	0.19	0.08	0.15	0.19	0.27	0.13	0.22	0.11	0.18	0.16	19
PROCED	0.15	0.08	0.17	0.12	0.05	0.25	0.28	0.21	0.22	0.15	18
ASSES	0.06	0.19	0.19	0.21	0.05	0.10	0.11	0.34	0.26	0.14	16
DOCUM	0.18	0.02	0.21	0.08	0.26	0.29	0.07	0.09	0.21	0.12	14
PARTNERS	0.08	0.49	0.14	0.14	0.13	0.15	0.02	0.13	0.06	0.11	13
C.R.	0.07	0.18	0.08	0.11	0.12	0.08	0.10	0.04	0.14	Average C.R.	0.09

APPENDIX 4. NON-RESPONSE BIAS TEST

The below table shows the results of ANOVA test performed at the 5 percent significance level in order to find if there is a significant difference between five sets of the returned questionnaires, specifically, piloting, the first mail-out, the first reminder, the second reminder and the third reminder.

Measurement Items	Sets of Respondents										Sig.
	1		2		3		4		5		
	Mean	Std. Dev.	Mean	Std. Dev	Mean	Std. Dev	Mean	Std. Dev	Mean	Std. Dev	
A11	4.36	0.81	4.44	0.69	4.47	0.51	4.21	0.63	4.38	0.52	0.69
A12	4.18	0.60	4.22	0.83	4.47	0.57	4.26	0.56	4.00	0.93	0.43
A13	3.91	0.83	4.00	0.89	4.00	0.91	3.68	1.11	3.18	1.13	0.12
A14	4.00	0.63	4.17	0.81	4.17	0.75	4.11	0.99	3.88	0.64	0.88
A15	3.91	0.83	4.22	0.76	4.47	0.57	4.21	0.63	4.50	0.53	0.15
A21	4.18	0.60	4.36	0.83	4.40	0.67	4.42	0.69	4.25	0.46	0.90
A22	4.45	0.52	4.39	0.60	4.37	0.61	4.47	0.84	3.88	0.83	0.29
A23	3.91	0.70	3.81	0.82	4.03	0.76	3.79	0.85	3.63	0.52	0.64
A24	4.00	0.45	4.00	0.76	4.17	0.65	4.00	0.58	3.75	0.71	0.59
A25	3.45	0.69	3.72	0.74	3.87	0.82	3.68	0.82	3.25	1.39	0.35
A26	4.27	0.47	4.25	0.73	4.13	0.73	4.21	0.54	4.38	0.52	0.89
A27	3.82	0.75	3.86	0.72	3.90	0.88	4.16	0.60	4.13	0.83	0.60
A28	2.55	0.82	3.06	1.01	3.33	1.21	2.95	1.18	2.38	1.06	0.12
A31	4.09	0.70	4.31	0.71	4.37	0.61	4.16	0.69	4.13	1.13	0.72
A32	4.09	0.70	4.14	0.64	4.43	0.57	4.22	0.71	4.00	0.93	0.30
A33	4.18	0.75	3.94	0.83	4.30	0.60	4.11	0.94	4.25	0.46	0.42
A34	4.09	0.70	4.06	0.75	4.33	0.66	4.00	0.88	3.63	1.19	0.21

A35	4.36	0.50	4.06	0.63	4.45	0.56	4.21	0.98	3.75	1.16	0.08
A36	4.18	0.40	4.03	0.70	4.13	0.78	3.84	0.96	3.50	0.53	0.20
A37	3.09	1.22	3.19	1.09	3.53	1.04	3.26	1.28	2.63	1.06	0.33
A38	3.09	1.22	3.00	1.07	3.43	1.14	3.05	1.43	2.75	1.16	0.51
A41	4.18	0.60	4.25	0.65	4.27	0.69	4.32	0.67	3.50	1.07	0.07
A42	4.09	0.70	4.37	0.64	4.21	0.71	4.42	0.69	3.75	1.04	0.16
A43	4.27	0.65	4.44	0.65	4.30	0.75	4.37	0.96	3.88	0.83	0.43
A44	3.91	0.70	4.11	0.82	4.17	0.87	3.95	0.85	4.00	0.93	0.85
A45	3.73	0.79	3.97	0.84	4.17	0.70	4.00	1.05	3.75	0.89	0.56
A51	4.27	0.79	4.25	0.65	4.13	0.78	4.26	0.73	4.25	0.46	0.96
A52	4.18	0.40	4.11	0.75	4.30	0.65	4.16	0.76	3.88	0.99	0.64
A53	4.09	0.70	3.75	0.97	4.10	0.71	4.00	0.88	4.00	0.53	0.49
A54	4.09	0.70	3.94	0.67	4.13	0.63	4.05	0.78	4.13	0.35	0.82
A55	4.18	0.75	4.03	0.77	4.03	0.72	4.00	0.88	4.13	0.35	0.97
A56	4.18	0.60	4.03	0.81	4.13	0.68	4.05	0.97	4.25	0.46	0.93
A61	3.82	0.75	4.08	0.69	4.07	0.74	3.79	0.98	3.63	1.19	0.43
A62	3.64	0.92	3.78	0.80	3.73	0.78	3.74	1.05	3.75	0.71	0.99
A63	3.45	0.69	3.39	0.93	3.73	0.87	3.74	1.05	3.13	1.13	0.32
A64	2.91	1.04	3.65	0.89	3.67	0.99	3.47	1.12	3.13	1.36	0.18
A65	3.73	1.19	4.14	0.76	4.20	0.76	4.21	0.54	3.88	0.64	0.39
A66	3.45	1.13	3.64	0.87	3.87	0.94	3.47	1.31	3.25	1.04	0.48
A71	4.09	0.70	4.17	0.70	4.10	0.80	4.05	0.85	4.00	0.53	0.97
A72	3.82	0.75	3.74	0.87	3.96	0.77	3.89	0.99	3.88	0.64	0.88
A73	4.18	0.60	3.89	0.82	4.23	0.63	4.11	0.94	3.88	0.99	0.42
A74	3.09	1.14	3.31	0.89	3.54	1.13	3.47	1.31	3.00	1.20	0.62
A81	4.00	0.63	3.89	0.78	4.03	0.67	3.95	1.13	4.00	0.53	0.96
A82	4.27	0.79	4.06	0.71	4.27	0.58	4.21	0.79	4.00	0.76	0.69
A83	4.27	0.90	4.08	0.84	4.13	0.68	4.21	0.71	3.75	0.89	0.64
A84	4.00	0.89	3.69	0.85	3.90	0.71	3.89	0.99	3.25	1.04	0.29

A85	3.82	0.87	3.77	0.76	3.87	0.78	3.74	1.24	3.00	1.07	0.20
A86	4.36	0.50	4.25	0.81	4.30	0.70	4.37	0.76	4.00	0.76	0.80
A91	2.91	1.14	3.14	0.96	3.61	1.00	3.37	1.30	2.75	0.71	0.14
A92	3.09	1.04	3.28	0.94	3.51	1.00	3.37	1.38	2.88	1.13	0.58
A93	3.09	1.22	3.36	1.10	3.81	0.88	3.49	1.21	3.13	1.13	0.24
A94	3.55	1.13	3.42	0.87	3.85	0.82	3.63	1.07	3.13	0.83	0.23
A95	3.09	1.04	3.49	0.73	3.82	0.70	3.42	1.30	3.13	1.13	0.13
B11	4.03	0.85	3.54	0.70	3.72	0.58	3.52	0.47	3.70	0.33	0.18
B12	3.97	0.90	3.62	0.95	3.78	0.54	3.65	0.60	3.68	0.87	0.72
B13	4.06	1.05	3.71	0.88	3.56	0.79	3.70	0.91	3.71	0.88	0.62
B14	3.72	0.87	3.55	0.70	3.64	0.64	3.68	0.65	3.69	0.33	0.92
B15	3.93	0.91	3.46	0.68	3.61	0.82	3.69	0.73	3.60	0.41	0.45
B16	3.78	0.85	3.52	0.81	3.38	0.73	3.57	0.44	3.57	0.42	0.59
B17	3.92	0.66	3.49	0.78	3.63	0.74	3.41	0.64	3.57	0.49	0.38
B18	1.96	0.85	2.57	0.99	2.51	0.59	2.75	0.90	2.94	0.77	0.09
B19	3.09	1.76	3.76	1.20	3.39	1.06	4.00	0.82	3.70	0.88	0.20
B21	3.09	1.30	3.22	0.87	2.77	0.97	2.84	1.07	2.88	0.99	0.40
B22	3.09	1.30	3.28	0.88	2.87	1.01	2.84	1.17	2.63	0.92	0.31
B23	3.10	1.30	3.25	0.92	3.07	0.91	2.92	1.15	2.88	0.64	0.76
B24	3.28	1.19	3.15	0.78	3.04	0.67	3.08	1.03	2.90	0.65	0.87
B31	3.07	0.95	2.86	0.47	2.99	0.47	2.64	0.61	2.65	0.40	0.13
B32	2.55	0.78	2.69	0.45	2.71	0.47	2.68	0.39	2.50	0.31	0.72
B33	3.32	1.10	3.62	0.73	3.52	0.69	3.45	0.64	3.51	0.85	0.83
B34	3.17	1.03	3.58	0.73	3.54	0.77	3.49	0.73	3.74	0.60	0.10
B35	2.98	0.51	3.51	0.66	3.28	0.75	3.29	0.48	2.89	0.56	0.08
B36	2.98	0.90	2.73	0.82	2.70	0.53	2.67	0.79	2.78	0.34	0.83
B37	2.36	0.50	2.52	0.78	2.55	0.57	2.70	0.71	2.64	0.44	0.74
B38	2.99	0.95	2.39	0.60	2.70	0.70	2.89	0.83	2.33	0.47	0.08
B39	2.97	0.64	2.48	0.87	2.68	0.72	2.61	0.80	2.78	0.36	0.41

B310	2.27	1.27	1.75	0.77	2.17	1.05	2.26	0.93	2.01	0.53	0.23
B311	2.55	0.65	2.42	0.78	2.48	0.70	2.53	0.79	2.88	0.58	0.62
B312	3.05	0.91	3.67	0.72	3.42	0.78	3.66	0.60	3.31	0.37	0.09
B313	2.83	0.61	3.21	0.50	3.15	0.48	3.25	0.70	3.18	0.63	0.34
B314	2.94	0.71	3.38	0.66	3.48	0.66	3.35	0.66	3.38	0.41	0.24
B315	2.82	0.60	3.30	0.59	3.27	0.72	3.39	0.82	3.06	0.55	0.19
B316	3.27	0.65	3.49	0.72	3.49	0.76	3.35	0.64	2.98	0.69	0.36
B317	3.13	0.71	3.50	0.63	3.52	0.75	3.47	0.75	2.98	0.69	0.19
B318	3.32	0.46	3.62	0.59	3.48	0.61	3.45	0.57	3.25	0.38	0.35
B319	3.22	0.60	3.53	0.65	3.46	0.60	3.44	0.57	3.23	0.37	0.54